Solution design
Nuts x AORTA/LSP

Datum:	06-02-2026
Status:	Concept / Vertrouwelijk
Versie:	0.1
Classificatie:	Klankboard document ter bespreking
Eigenaar:	xxx
Revisie:	

1 Wijzigingenblad

Versie	Datum	Omschrijving	Auteur
0.1			
0.2			
0.3			
0.4			
0.5			

2 Inleiding

2.1 Context

In 2023 sprak het Ministerie van VWS (hierna: VWS) de wens uit om Twiin, Nuts, LSP (VZVZ) en (optioneel) Zorgplatform met elkaar te verbinden, om zo de basis te leggen voor een landelijk dekkend netwerk – het Landelijk Dekkend Netwerk (hierna: LDN). VWS verzocht de betrokken partijen om, in lijn met deze wens, hun eigen initiatieven te formuleren.

Een belangrijke succesfactor voor het realiseren van het LDN is het onderlinge vertrouwen tussen de betrokken partijen: vertrouwen dat wordt omgezet in afspraken, juridische en technologische waarborgen en specificaties. In de loop van 2023/2024 zijn diverse projecten en programma's gestart om de stappen te definiëren (initiatieven, werkpakketten en benodigde afspraken) die moeten leiden tot een landelijk vertrouwensecosysteem – het Landelijk Vertrouwensstelsel (hierna: LVS).

Deze werkpakketten – waaronder de Interface Nuts x LSP x Zorgplatform – zijn vervolgens ondergebracht bij de VWS-programma's LDN en Implementatie Generieke Functies (IGF). Rond deze periode wees VWS ook Twiin aan als uitvoeringsorganisatie voor het LVS, later omgevormd tot het Programma Transitie Landelijk Afsprakenstelsel (LAS). Om die reden staat het project Koppeling Nuts x LSP in nauwe relatie tot Twiin/LAS en VWS.

2.2 Aanleiding

Actiz heeft sinds 2020 aandacht gevraagd voor de koppeling Nuts met AORTA/LSP. Toen reeds waren er plannen, maar die zijn om verschillende redenen niet ten uitvoer genomen. De wens voor een dergelijk koppeling is echter niet verdwenen. Vanuit AORTA zijn meerdere pogingen gedaan om dit onderzoek vlot te trekken.

In februari 2025 startte het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) een Proof of Concept (PoC) met de titel PoC Nuts x LSP. Het primaire doel van deze PoC was het ontwerpen en testen van de technische infrastructuur die nodig is om gegevensuitwisseling tussen beide netwerken mogelijk te maken, met gebruikmaking van de Generieke Functies (GF's).

Kort na de start van de PoC sprak het regionale netwerk REN West-Brabant de ambitie uit om verder te gaan dan een puur experimentele opzet en een oplossing te realiseren die geschikt is voor productiegebruik. Hierdoor werd de scope van het project verbreed: naast een PoC werd ook een pilotfase toegevoegd.

Tijdens de opstartfase ontwikkelden architecten van Twiin, Nuts, VWS en VZVZ gezamenlijk een Project Start Architectuur (PSA). Uit deze architectuuranalyse kwamen verschillende knelpunten naar voren die verdere uitwerking en besluitvorming vereisten. De ambitie om op korte termijn richting productie te bewegen bracht extra complexiteit met zich mee:

- architectuuroplossingen moesten binnen beperkte tijd een hoger volwassenheidsniveau bereiken;
- enkele noodzakelijke componenten (zoals onderdelen van de Generieke Functies) bevinden zich nog in de ontwerpfase en zouden binnen de beschikbare tijd niet de benodigde productievolwassenheid kunnen bereiken.

Op basis van deze bevindingen concludeerden VWS, Nuts en VZVZ (namens Twiin en LSP) gezamenlijk dat het te complex was om zowel de volledige toepassing van de Generieke Functies uit te werken als deze oplossingen binnen korte tijd in productie te brengen. Daarom werd besloten het initiatief op te splitsen in twee complementaire, parallelle en convergerende trajecten:

- Een kortetermijnproject - Interface Nuts x LSP (door Nuts and VZVZ) - Gericht op het op korte termijn mogelijk maken van gegevensuitwisseling tussen Nuts en LSP, geschikt voor gebruik in zowel pilot- als productieomgevingen.

- Een langetermijnproject - (PoC 12 LSP x VVT (door VWS) - Gericht op het verder uitwerken van de toepassing van de Generieke Functies, voortbouwend op en uitbreidend ten opzichte van de kortetermijnoplossing, en aansluitend bij toekomstige ontwikkelingen.

2.3 Doelstelling

Dit project heeft als doel:

- een ontwerp te maken van een bi-directionele koppeling tussen AORTA/LSP en Nuts inclusief de mogelijkheid om gespreid bevragen door AORTA/LSP;
- met draagvlak binnen Nuts en VZVZ en in lijn met landelijke ontwikkelingen zoals Twiin en LDN (VWS);
- de koppeling te realiseren met leveranciers en beproeven in een test- en later in een productieomgeving om bevindingen en aanbevelingen te verzamelen;
- Het creëren van de randvoorwaarden om verdere uitrol mogelijk te maken;
- Het uitwerken van een vertrouwensmodel op basis van Twiin of AORTA op welk de uitwisseling plaatsvindt;
- om zo tot een blijvende gegevensuitwisseling van een concrete bestaande zorgtoepassing te komen.

2.3.1 Beoogde resultaten

Het project streeft de volgende resultaten na:

- Een ontwerp en realisatie van de koppeling tussen Nuts en LSP conform gestelde randvoorwaarden dat wordt gedragen door VZVZ en Stichting Nuts. Dit omvat onder meer:
  - een werkende bi-directionele koppeling tussen Nuts en het LSP;
  - het LSP is in staat om op Nuts aangesloten zorgaanbieders te bevragen middels een gespreide bevraging (agnostisch)
  - het vertrouwen is uitgewerkt in een release candidate (beproefde bèta versie) die opgenomen is/wordt in het Twiin of AORTA Afsprakenstelsel
  - een gewijzigde infrastructuur van AORTA/LSP en Nuts
  - een werkend Nuts-GtK in productie

- We volgen het volwassenheidsmodel; ontwerpkeuzes leggen we voor aan relevante stakeholders.
  - opgehaald tijdens drie klankbordsessies gedurende het project met bijzondere aandacht voor effecten op processen, infrastructuur en governance, en inbreng vanuit Twiin standaardisatie.
  - inclusief het formuleren en uitzetten van eventuele vervolgacties (bij Nuts- of VZVZ-collega's) om impact te mitigeren t.b.v. de pilot en latere release, of om draagvlak te vergroten onder stakeholders.
  - het bespreken van ontwerpkeuzes tijdens de TPA
  - afstemming met relevante projecten, uitwerkingen en realisaties van onder andere Twiin, VWS (LDN, PoC 12 LSPxVVT, DEZI).

- Een beproeving van het gerealiseerde ontwerp waarbij bevindingen en aanbevelingen zijn opgehaald ter verbetering van het ontwerp middels:
  - het uitvoeren van een tweetal PoC's (NUTS bevraagt LSP, LSP bevraagt NUTS) in een referentieomgeving;
  - het uitvoeren van een tweetal pilots (NUTS bevraagt LSP, LSP bevraagt NUTS) in een productieomgeving met eindgebruikers en een concrete zorgtoepassing met speciale aandacht voor de verificatie van juridische, technische en functionele randvoorwaarden, en logging, toestemming, governance en vertrouwen.

- Een rapportage van bovenstaande beoogde resultaten met daarin een verslag van
  - het uitgevoerde project, bevindingen en aanbevelingen en behaalde resultaten
  - gerealiseerde ontwerpen met benodigde toelichting

- aanbevelingen voor besluitvorming over landelijke uitrol en structurele borging van de gerealiseerde gegevensuitwisseling
- indien pilots worden doorgeschoven naar een separaat project: voorstel voor doorontwikkeling richting tweerichtingsverkeer.

2.4 Kaders

2.4.1 Uitgangspunten

- Leveranciers worden betrokken gedurende het project. In de PoC fases kan dit nog in mindere mate zijn om snelheid te maken. Tijdens de pilot is dit afhankelijk van de aangemelde samenwerkingsverbanden (uit het veld) die willen deelnemen aan de pilots
- Onderzocht wordt hoe we verder samen werken met Twiin en hoe we het vertrouwensmodel anders of aanvullend kunnen vormgeven, zodat beide trajecten goed op elkaar aansluiten.

2.4.2 Randvoorwaarden

- We ontwikkelen op onze eigen kracht en op ons eigen tempo. Dat betekent dat we aansluiting zoeken bij landelijke initiatieven maar ons daar niet afhankelijk van maken.
- De koppeling voorziet in bi-directioneel verkeer tussen Nuts en AORTA. De koppeling is use case agnostisch. De gehanteerde use cases in de pilots worden afgestemd met de deelnemende partijen aan deze pilots.
- Nuts en LSP worden gekoppeld via een in dit project te ontwikkelen boven op de bestaande LSP-GtK die communiceert met een Nuts-GtK (dat kunnen er meerdere zijn).
- Nuts en VZVZ werken gezamenlijk in een multidisciplinair team, waarbij beide organisaties expertise en capaciteit inbrengen. Hierdoor is gewaarborgd dat de benodigde kennis op het juiste moment beschikbaar is om inhoudelijke en organisatorische vraagstukken adequaat te adresseren.
- We conformeren ons aan landelijke ontwikkelingen zoals het werkpakket LDN Nuts x AORTA/LSP
- Waar generieke functies beschikbaar zijn, worden deze benut, zo lang als dit de voortgang en uitvoerbaarheid van het project niet onevenredig belemmert

2.4.3 Buiten scope

- De ontwikkeling van nieuwe zorgtoepassingen
- Opschaling naar productie
- Uitbreiding met patiënt perspectief

2.5 Deelnemers & Stakeholders

Stakeholder	R	A	S	C	I	toelichting
Stichting Nuts	●	●				Trekkers project
AORTA/ZORG-ID (VZVZ)	●	●				Trekkers project
Itzos			●	●		Leverancier van VZVZ
AET Europe			●	●		Leverancier van VZVZ
Het Ministerie van VWS				●	●	Organiseert aanverwante projecten
Twiin (VZVZ)	(●)		(●)	●	●	Stelsel waar oplossing in zou moeten passen
Stichting Gemeenschappelijke Voorzieningen voor Zorgcommunicatie (GVvZ)			(●)	●	●	
Management/Directie VZVZ					●	
Overige VZVZ-afdelingen			(●)	●	●	
Zorgaanbieders	●			●	●	Deelnemer Pilots
Leveranciers	●			●	●	Deelnemer Pilots (en PoC's)
Zorgverzekeraars Nederland (ZN)					●	Financier VZVZ
ActiZ (en andere branchorganisaties/koepels)					●	Vertegenwoordigen zorgaanbieders

3 Voorgeschiedenis & aanpalende ontwikkelingen

3.1 Eerdere trajecten

Na het verzoek van Actiz aan VZVZ is dit project lang op de bestuurlijke tafels blijven liggen, omdat een oplossing niet direct voor handen leek te liggen. Ook tijdens de COVID-periode zijn verschillende opties ter realisatie besproken.

Er zijn verschillende trajecten doorlopen, zoals:

1. Twiin formaliseert het koppelen van afsprakenstelsels. Twiin is echter nog niet ver genoeg om daadwerkelijk te koppelen. Wel is er door Twiin een onderzoek gedaan tot de vereisten voor landelijke gegevensuitwisseling en de route die Nuts moet doorlopen om aan deze eisen te voldoen.
2. Het project 'Generieke Functies' heeft zich gericht op de adressering. Ook is er gewerkt aan de 'TA (Technical Agreement) notified pull, waarbij VC's van Nuts worden ingezet.
   Voor Adressering is er in 2024 een hackathon Nuts x LSP geweest.

3.2 Belangrijke besluiten uit het verleden

'Voortborduren op beslissingen die in het verleden genomen zijn'. Het aansluiten van afsprakenstelsels op Twiin heeft als doel om gedane investeringen niet te vernietigen, maar juist in te zetten om verder te groeien.

Uitgangspunt is dat de GtKen (Gekwalificeerde Twiin Knooppunten) de 'verschillen' tussen de afsprakenstelsels overbruggen. Één onderwerp laat zich echter niet overbruggen en dat is het 'Vertrouwen'. Omdat alle deelnemende afsprakenstelsels binnen Twiin hiervoor een oplossing nodig hebben, is ervoor gekozen voor een duale oplossing: binnen het afsprakenstelsel wordt gebruik gemaakt van de 'eigen' afspraken, maar voor communicatie via Twiin, zullen voor de deelnemers (zorgaanbieders) generieke VCs worden uitgewisseld (basis bouwblokken), die per use-case (toepassing) worden gedefiniëerd. De invulling van de VC's is erop gericht ze in alle contexten te kunnen toepassen, zowel binnen een afsprakenstelsel als daarbuiten.

De ambitie om het netwerk van NUTS te koppelen aan het AORTA Afsprakenstelsel via het Landelijk Schakelpunt (LSP) is niet nieuw. In een eerder stadium is tijdens een designathon al verkend hoe dit kan. Deze verkenning is de eerste aanzet geweest tot een technisch en functioneel haalbaarheidskader. Hierbij wordt via GtKen gecommuniceerd, zodat 'later' ook andere afsprakenstelsels op gelijke wijze kunnen worden gekoppeld.

Belangrijke conclusies uit hackathon Nuts x LSP. De VC-adressering zou uitgegeven kunnen gaan worden door ZORG-AB, zolang het 'Landelijke Adresboek' nog niet beschikbaar dan wel gevuld is.

Twiin wordt de landingsplaats voor afspraken over de afsprakenstelsels heen.

Het gebruik van Generieke Functies wordt door Twiin, Nuts én AORTA bevorderd, maar zal niet dwingend zijn als deze (nog) niet op het noodzakelijke niveau beschikbaar zijn

In de aanloop naar dit project heeft afstemming op hoofdlijnen plaatsgevonden met architecten van zowel VZVZ als NUTS en Twiin. Op basis van deze gesprekken en de eerder uitgevoerde designathon is vastgesteld dat een koppeling tussen NUTS en het LSP technisch haalbaar lijkt.

3.3 Aanpalende ontwikkelingen

Om tot een duurzame oplossing te komen wordt afstemming en aansluiting gezocht bij landelijke ontwikkelingen.

3.3.1 Samenhang en afhankelijkheden

Vanuit het Landelijk Vertrouwensstelsel (LVS) is een werkpakket gedefinieerd dat voorziet in het aan elkaar koppelen van de infrastructuren van NUTS en LSP. Dit werkpakket is nu in beheer bij het Landelijk Dekkend Netwerk. Het LDN is voornemens om het werkpakket op te gaan pakken na afronding van het werkpakket Veilig Netwerk. De te realiseren koppeling zal in het kader van dit werkpakket worden uitgevoerd. Hierbij zal de uitwisseling tussen de twee infrastructuren gebeuren op basis van de Gevalideerd Twiin Knooppunt (GtK) route waarbij het vertrouwen door het Twiin afsprakenstelsel wordt geleverd.

Een belangrijk deel van het koppelen van NUTS en AORTA/LSP, is de identificatie en authenticatie (I&A) van de zorgaanbieder en de zorgverlener. Hier is het team Generieke Functies (GF) van VWS mee bezig onder de naam Dé Zorgidentiteit, afgekort DEZI. DEZI wordt door VWS ontwikkeld om zorgverleners en -aanbieders in het gehele zorgveld de mogelijkheid te bieden zich veilig en betrouwbaar te identificeren en authenticeren.

Samen met betrokken architecten van GF, VZVZ (AORTA/LSP en Twiin) en NUTS is een PoC gedefinieerd om de randvoorwaarden voor I&A en andere generieke functies verder uit te werken. Ook Twiin is hierbij betrokken. Binnen dit project worden generieke functies, zoals DEZI, lokalisatie, autorisatie, adressering en logging, benut en, waar nodig, verder doorontwikkeld om ze geschikt te maken voor deze specifieke koppeling en toekomstige herbruikbaarheid. Deze PoC kent meerdere benamingen zoals PoC LSPxNUTS, PoC LSPxVVT. Wij noemen hem hier PoC DEZI.

Onder regie van Twiin wordt gewerkt aan een Technical Agreement voor Pull-uitwisselingen (TA Pull), waarbij ook VZVZ actief is betrokken. Een van de onderwerpen binnen deze TA Pull is I&A.

Er is nog weinig zicht op definitieve tijdslijnen van de genoemde initiatieven. Mogelijk lopen de agenda's voor op die van Twiin en het LDN. Zowel vanuit Twiin als vanuit VWS LDN is mondeling aangegeven dat men bereid is samen te werken. Hierdoor kan het voorkomen dat projecten beide ontwikkelingen in een ander tempo worden vormgegeven, maar later zullen worden samengevoegd voor het beoogde eindresultaat.

3.3.2 Afstemming met andere ontwikkelingen

Afstemming tussen deze projecten vindt continu plaats:

- De **PoC 12 LSP x VVT** ,(VWS) beproeft de generieke functies toepast op een koppeling tussen het Nuts-netwerk en het LSP voor de toekomstige situatie waar landelijk wordt gewerkt met de generieke functies. Dit project voor de Koppeling Nuts x LSP is de opmaat naar deze toekomstige situatie. Met deze PoC vindt directe coördinatie plaats binnen het Nuts x LSP-projectteam, waarvan de teamleden ook deelnemen aan PoC LSP x VVT.
- Met **Twiin** (en haar werkgroepen omtrent de Technical Agreement Notified Pull (TA NP)) om te zorgen dat de koppeling zo veel mogelijk berust op concepten uit, geschikt voor of in lijn met het Twiin Afsprakenstelsel. Deze koppeling kan daarmee op termijn worden ondergebracht in Twiin en later in het Landelijk Afsprakenstelsel.

Met Twiin en VWS organiseren we wederzijdse reviews van specificaties met als doelstellingen:

- het voorkomen van desinvesteringen,
- het waarborgen van architecturale consistentie, en
- het vaststellen van een duidelijke groeilijn van Nuts x LSP, naar LSP x VVT, en uiteindelijk richting de LAS.

Ook volgen we de ontwikkelingen bij Nictiz over de Informatiestandaard Lokalisatie. Deze standaard is nodig om lokalisatiegegevens tussen Nuts en AORTA te kunnen uitwisselen zodat de zorgaanbieders met gegevens van de patiënt kunnen worden gevonden.

3.4 Conclusies

Het project Nuts x AORTA/LSP zal de verbinding leggen tussen beide afsprakenstelsels op basis van de huidige mogelijkheden, waarbij de resultaten van dit project zullen worden afgestemd en vastgelegd binnen het Twiin-afsprakenstelsel.

Gezien de wens tot realisatie van een oplossing én het inzicht dat vertrouwen zich niet laat vertalen is ervoor gekozen voor het onderwerp Identificatie en Authenticatie, waaronder ook de waarborgen voor gegevensuitwisseling vallen, om een generieke afspraak voor I&A op te stellen voor zowel Nuts als AORTA, waar bij stelsels een hybride vorm van afhandeling van waarborgen zullen gaan bevatten.

Deze generieke afspraak voor I&A is een infrastructurele afspraak, dus onafhankelijk van welke zorgtoepassing dan ook.

4 Aanpak, fases en opzet

GtK
In dit document bedoelen we met een GtK de infrastructurele component. Als deze niet gevalideerd is op het moment van oplevering, dan is er vanuit LSP-perspectief sprake van een Goed Beheerde Connector (GBC).

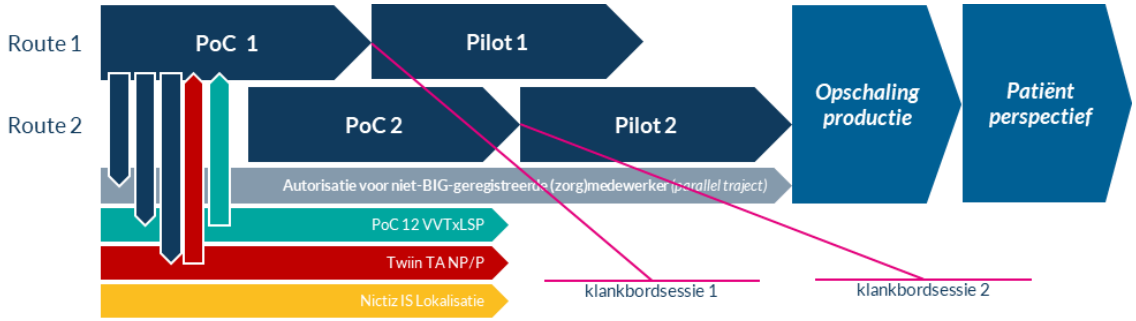
4.1 Aanpak

Tijdens de ontwikkeling van de koppeling is de stip op de horizon dat de communicatie via een Gevalideerd Twiin Knooppunt (GtK) verloopt. Daarom bouwen we vanuit het LSP boven op onze bestaande LSP-GtK. Nuts ontwikkelt aan haar open-source component waarbij deze onderdeel kan zijn van een Gevalideerd Twiin Knooppunt.

We specificeren en bouwen tegelijkertijd. Zowel aan de Nuts kant als aan de kant van het LSP. We werken kort cyclisch en directief. Sourcing partners zijn onderdeel van het ontwikkelteam. De realisatie van de koppeling tussen Nuts en LSP verloopt gefaseerd. Zo verhogen we stapsgewijs de volwassenheid van de oplossing. We hanteren twee routes voor de gegevensuitwisseling, en meerdere fases voor de uitvoering.

4.1.1 Routes & fasering

- Route 1: Nuts bevraagt LSP
- Route 2: LSP bevraagt Nuts



De uitvoering ziet er als volgt uit:

- Het voortbrengingsproces wordt gevolgd met behulp van expertsessies, klankbordgroep, PoC en Pilots.
- Het project kent de volgende fasen:
  - PoC 1 - NUTS bevraagt het LSP (in afronding)
  - Pilot 1 - NUTS bevraagt het LSP
  - PoC 2 – LSP bevraagt NUTS
  - Pilot 2 – LSP bevraagt het LSP
  - Vertrouwensmodel
  - Autorisatie niet-BIG geregistreerden
- Om tot een duurzame oplossing te komen wordt afstemming en aansluiting gezocht bij landelijke ontwikkelingen:
  - PoC 12 VVTxLSP
  - Twiin TA NP
  - Nictiz ontwikkeling informatiestandaard lokalisatie
- Fasen kunnen parallel verlopen. We streven ernaar dat hierdoor geen dubbel werk ontstaat.
- Als vervolg zien wij 1) opschaling naar productie en 2) uitbreiding van LSP+ om bevraging door de patiënt via het LSP mogelijk te maken.

4.2 Toelichting fases

De realisatie van de koppeling tussen Nuts en LSP verloopt gefaseerd. Zo verhogen we stapsgewijs de volwassenheid van de oplossing. Hiervoor passen we het Voortbrengingsproces toe.

4.2.1 Voortbrengingsproces (volwassenheidsmodel)

Om duurzame oplossingen te bouwen is het noodzakelijk die tijdens de verschillende fasen voor te leggen aan relevante stakeholders waaronder leveranciers, zorgaanbieders, koepels, VWS, Twiin etc. Wij hanteren de volgende methodiek:

- Expertsessies: tijdens het TPA bespreken we de ontwerpen met leveranciers;
- Klankbordsessies: een afspiegeling van relevante stakeholders geeft feedback op het functioneel en technisch ontwerp tijdens/na de PoC en Pilot fases.
- PoC's: beproeving van de koppeling in een referentieomgeving.
- Pilot: beproeving van de koppeling in een productieomgeving

4.2.2 Fase 1: PoC Nuts bevraagt LSP

In de PoC willen we de flow beproeven van het opvragen van een (medicatie) resource op het LSP door een XIS in een referentieomgeving. Nuts past haar open source component aan en het LSP past haar infrastructuur aan. Tijdens een aantal ontwerpsessies specificeren we de te ontwikkelen koppeling. Hoofdonderdelen zijn identificatie en authenticatie middels verifiable credentials.

4.2.3 Fase 2: PoC LSP bevraagt Nuts

We ontwikkelen en beproeven de flow waarbij Nuts wordt gevraagd vanuit het LSP voor een nog nader te bepalen zorgtoepassing/informatiestandaard. Hierbij moet het voor het LSP agnostisch zijn of een partij via Nuts of het LSP is aangesloten: we bieden dezelfde ervaring. Dit betekent dat in deze fase gemeenschappelijke voorzieningen waaronder I&A, toestemmingen, adressering en (lokalisatie) onderdeel zijn van de ontwikkeling

4.2.4 Fase 3: Pilot Nuts bevraagt LSP

We maken de PoC brengen deze naar productie. Hierbij werken we naast het vertrouwen ook de lokalisatie uit op basis van Mitz. Vervolgens beproeven we de koppeling in productie. Daarbij bevraagt het Nuts-netwerk het LSP voor een nader te bepalen zorgtoepassing. Het identificatiemiddel tijdens de pilot is de UZI-pas.
Deze fase begint met het ontwikkelen van de ontbrekende schakels om naar 'productie' te gaan met een GtK. Hiervoor ontbreekt nog een credential in de PoC1 fase. Ook zal de documentatie en testen op niveau worden gebracht om verantwoord in productie te gaan.

4.2.5 Fase 4: Pilot LSP bevraagt Nuts

We maken de PoC ontwikkelingen productierijp en brengen deze naar productie waar we de koppeling beproeven in een praktijksituatie in de vorm van een pilot.

4.2.6 Vertrouwensmodel

Ten behoeve van de uitwisseling is het noodzakelijk dat de uitwisseling plaats vindt onder vertrouwen wat op twee manieren realiseerbaar is: via Twiin en via AORTA. Het uitwisselen via Twiin is het doel. Mocht Twiin dit vertrouwen niet (tijdig) kunnen formaliseren in haar afsprakenstelsel, dan kiezen we voor een (al dan niet tijdelijke) invulling vanuit AORTA. Daarbij kiezen we zo veel mogelijk voor verwijzen naar Twiin en verschaffen we een aanvullend kader.

Twiin en AORTA zijn **de realisatie van het abstracte "issuer trusted by verifier" principe** in de praktijk. De cryptografie van VC/VP blijft hetzelfde; wat verandert, is **wie als vertrouwde issuer wordt erkend**.

4.2.7 Autorisatie niet-BIG geregistreerden

Voor zorgverleners zonder BIG-registratie is geen autorisatieprofiel beschikbaar. Hierdoor beschikken zij niet over de benodigde BIG-gebaseerde rolcodes om bepaalde gegevens op te halen waarmee zij in staat zijn gerichte (medische) handelingen te verrichten. Dit komt veel voor in de VVT en gehandicaptenzorg, maar ook in andere sectoren. Voor de opschaling in (onder meer) de VVT is het noodzakelijk dat dat dit wel

geregeld is. We voorzien een oplossing waarbij zorgaanbieders zelf identiteiten en taak/rolcodes kan uitgeven.

5 Nuts x AORTA/LSP – IST

Leeswijzer hoofdstuk

5.1 Huidige situatie

De gegevensuitwisseling in de zorg is momenteel beperkt tot op zichzelf staande systemen en infrastructuren. Zorgaanbieders kunnen alleen gegevens uitwisselen met andere zorgaanbieders die van hetzelfde systeem of infrastructuur gebruikmaken. Er is geen overkoepelende infrastructuur die deze systemen en/of infrastructuren met elkaar verbindt.

In de huidige situatie zijn de gegevensuitwisselingen dus beperkt tot het systeem of de infrastructuur waarop de zorgaanbieders zijn aangesloten. Echter in het geval van de VVT-sector, is er behoefte om medicatieoverzichten van cliënten (patiënten) te kunnen inzien bij de apotheker en/of huisarts. Dit is momenteel niet mogelijk aangezien deze zorgaanbieders op verschillende infrastructuren zijn aangesloten.

5.1.1 Wet- & regelgeving

Ongeacht of de zorgaanbieders op dezelfde infrastructuur of op verschillende infrastructuren zijn aangesloten, moeten de opslag van medische gegevens en de gegevensuitwisselingen voldoen aan dezelfde wet- en regelgeving zoals:

- AVG / UAVG
  Bescherming van persoonsgegevens, rechtsgrond voor verwerking van bijzondere persoonsgegevens (gezondheidsgegevens), eisen aan toestemming, intrekking, dataminimalisatie, logging, DPIA.
- WGBO
  Patiënt heeft recht op inzage, toestemming en dossierbeheer; beroepsgeheim; wie mag gegevens inzien.
- Wabvpz
  Specifieke bepalingen voor elektronische uitwisseling; traceerbaarheid en logging; toestemming en audit van digitale gegevensuitwisseling.
- Wegiz + Regeling elektronische gegevensuitwisseling
  Verplicht elektronische uitwisseling bij aangewezen zorgaanbieders; aanwijzing van standaarden, gegevensets en koppelingen; borgt interoperabiliteit. In AMVB's wordt geregeld welke uitwisselingen verplicht zijn (MedicatieOverdracht, eOverdracht, BGZ, Beeldbeschikbaarheid).
- Wet BIG
  Toegang en bevoegdheid van zorgverleners, bepaalt wie welke medische gegevens mag verwerken.
- Wkkgz
  Kwaliteit en verantwoorde zorg; borgt correcte en veilige dossiervoering.
- Wbni / NIS2 implementatie
  Cybersecurity- en meldplicht; beheersmaatregelen voor vitale systemen.

5.1.2 Organisatie

De complexe en snel veranderende zorgsector vereist een naadloze, betrouwbare en veilige uitwisseling van medische gegevens. De aandachtspunten voor organisaties bij (elektronische) gegevensuitwisseling zijn:

- Identificatie: bepaald moet worden op basis van welke attributen organisaties en zorgverleners geïdentificeerd moeten worden, bijvoorbeeld aan de hand van een toegewezen rol of een nummer. Bij het vastleggen van patiëntgegevens (WID en SBV-Z gecontroleerd) en bij gegevensuitwisseling– en in Nederland is het verplicht om patiënten te identificeren op basis van het BSN. Bij de

uitwisseling van medische gegevens is het van belang dat er afspraken zijn over hoe personen, organisaties en bijvoorbeeld systemen worden geduid.

- Authenticatie: bij gegevensuitwisseling zijn afspraken nodig op basis waarvan authenticatie van personen en organisaties plaatsvindt. Het type uit te wisselen gegevens bepaalt de eisen die aan de betrouwbaarheid van het authenticatiemiddel wordt gesteld (leidend hierin is eIDAS).
- Autorisatie: voor uitwisselingen tussen zorgaanbieders moeten autorisatieafspraken worden gemaakt. De afspraken leggen vast (met) welke (rol een) zorgverlener toegang heeft tot bepaalde informatie. Gegevensuitwisselingen moeten proportioneel zijn en een bepaald doel hebben. Autorisatieafspraken geven hier invulling aan, zodat vastgesteld kan worden wie de autorisaties bepaalt (raadplegende zorgaanbieder, dossierhoudende zorgaanbieder of via landelijke afspraken) en waar deze autorisaties worden gecontroleerd (bij de raadplegende zorgaanbieder, bij dossierhoudende zorgaanbieder, regionaal of via een centrale voorziening).
- Behandelrelatie: een zorgverlener mag alleen toegang hebben tot (medische) gegevens, wanneer deze een behandelrelatie met de patiënt heeft. Dit geldt zowel voor zorgverleners die in hun eigen zorgorganisatie een dossier benaderen als voor zorgverleners die gegevens raadplegen bij een andere zorgaanbieder, via bijvoorbeeld een uitwisselingssysteem.
- Patiënttoestemming: bij elektronische uitwisseling van medische gegevens geldt dat de patiënt toestemming moet geven voor het beschikbaar stellen van zijn gegevens voor mogelijke raadpleging door een andere zorgaanbieder in de toekomst.
- Logging: logging maakt het mogelijk het beheer van uitwisselingen goed in te richten. Wanneer er technische problemen zijn bij het tot stand brengen van de uitwisseling kan via de logging nagegaan worden waar het probleem in de keten ligt. De andere functie van logging is dat logging van transacties het mogelijk maakt om te controleren of de uitwisselingen volgens de afspraken plaatsvinden. Dit betreft altijd controle achteraf. De NEN7513 regelt de structuur van de logging en toegang door de patiënt.
- Transparantie: transparantie omvat afspraken over hoe zorgaanbieders, zorgverleners en patiënten kunnen weten wat de afspraken over de waarborgen in het vertrouwensmodel zijn. Zorgverleners moeten op de hoogte zijn van het beleid op de waarborgen van het vertrouwensmodel, zowel intern als bij uitwisseling tussen zorgaanbieders. Voordat een zorgaanbieder uitwisselt met andere zorgaanbieders, moet deze op de hoogte zijn van de vastgelegde afspraken hierover. De zorgaanbieder zal, net als de andere deelnemende zorgaanbieders, aan de afspraken moeten voldoen.
- Lokalisatie: waarborgen ten aanzien van lokalisatie zijn nodig in het geval gegevens ongericht beschikbaar gesteld zijn voor opvragen. Ongericht beschikbaar stellen van gegevens houdt in dat gegevens na toestemming van de patiënt beschikbaar worden gesteld aan andere zorgorganisaties, zonder dat vooraf bekend is welke zorgorganisatie de gegevens op welk moment zal opvragen. Bij een aantal uitwisselingen is niet vooraf bekend welke gegevens de zorgverlener nodig heeft, zoals bij acute situaties, vrije keuze van zorgverlener door patiënt, ad hoc contacten (b.v. vakantie).
- Adressering: adressering is zowel noodzakelijk bij het ongericht beschikbaar stellen als bij het gericht versturen van informatie. Bij het gericht versturen van gegevens worden gegevens vanuit het systeem van de brondossierhouder direct naar een bekende ontvanger gestuurd. Hier geeft adressering antwoordt op de vraag, wat het “digitale adres” van de ontvanger is. Bij het ongericht beschikbaar stellen van gegevens geeft adressering de opvragende zorgaanbieder antwoord op de vraag wat het “digitale adres” van de bron is.
- Verantwoordelijkheden leveranciers: afspraken over SLA’s, beveiliging en naleving van wettelijke verplichtingen.
- Audit en compliance: interne controles, incidentmeldingen en documentatie voor toezichthouders (IGJ, AP).

Voor zorgaanbieders op het LSP zijn al deze punten geborgd in het AORTA-afsprakenstelsel en de architectuur van het LSP.

Nuts is geen volledig afsprakenstelsel. Het omvat een technisch architectuur waarin alleen identificatie, authenticatie en autorisatie zijn ingevuld.

5.1.3 Zorgproces

Wanneer in het zorgproces medische gegevens benodigd zijn van zorgaanbieders die aangesloten zijn op een andere infrastructuur, dan is het momenteel niet mogelijk om deze gegevens direct op een elektronische manier in het XIS te ontvangen.

In het geval dat een VVT-organisatie medicatiegegevens wil ontvangen van een zorgaanbieder op het LSP (of andersom), dan is het momenteel niet mogelijk om deze gegevens (automatisch) elektronisch uit te wisselen. Hierdoor wordt het zorgproces vertraagd en kan het mogelijk de patiëntveiligheid in gevaar brengen omdat de benodigde medicatiegegevens te laat of niet volledig beschikbaar zijn.

5.1.4 Informatie

Om te zorgen dat de gegevensuitwisseling kan plaatsvinden en dat deze gegevens opgeslagen kunnen worden in het XIS, moeten er afspraken worden gemaakt aan welke standaarden moeten worden voldaan.

Voor de huidige productie-omgeving van het LSP geldt dat de standaard voor medicatiegegevens MP6.12 is, waarbij de ondersteuning van en overgang naar MP9 wel in gang is gezet. Voor het LSP geldt dat beide standaarden worden ondersteund, maar omdat voor de meeste medicatiegegevens nog MP6.12 wordt gebruikt, wordt dit, indien nodig, getransformeerd naar MP9 en vice versa.

Nuts verzorgt vertrouwensdiensten en specificeert niet welke informatiestandaarden worden toegepast. De XIS-leveranciers in de VVT hebben afgesproken om de MP9-standaard in te bouwen. Zorgaanbieders in de VVT kunnen geen gebruik maken van een transformatiedienst om oudere berichten om te zetten naar MP9 (en vice versa).

5.1.5 Applicatie

De zorgaanbieder gebruikt voor de administratie van patiëntgegevens en het bijbehorende dossier een XIS. Het XIS moet alle (type) gegevens die bij de behandeling behoren kunnen opslaan. Ook moet het XIS deze gegevens beschikbaar kunnen stellen aan andere zorgaanbieders (indien de patiënt daar toestemming voor heeft gegeven) en/of de gewenste gegevens kunnen ontvangen van andere zorgaanbieders.
Het XIS moet dus alle (informatie)standaarden en formaten, die bij deze gegevensuitwisselingen behoren, ondersteunen. Daarnaast moet het XIS de functionaliteiten hebben om op de desbetreffende infrastructuur te kunnen communiceren.

Voor de zorgaanbieders die op het LSP zijn aangesloten geldt dat de meeste XIS'en de MP6.12 standaard wordt gebruikt. Leveranciers zijn bezig om de functionaliteit van de MP9-standaard in te bouwen, maar het is nog onbekend wat het tijdspad hiervoor is.

De XIS-leveranciers in de VVT hebben afgesproken om de MP9-standaard in te bouwen, onduidelijk is wanneer dit gerealiseerd is.

5.1.6 Infrastructuur

In het huidige zorgveld bestaan verschillende systemen en infrastructuren waar medische gegevens worden uitgewisseld, maar deze systemen en infrastructuren staan over het algemeen op zichzelf. Dit betekent dat deze medische gegevens alleen binnen het desbetreffende systeem of infrastructuur beschikbaar zijn en dus niet beschikbaar zijn voor zorgaanbieders die op een andere infrastructuur zijn aangesloten.

Voor AORTA/LSP geldt dat zorgaanbieders die onderling gegevens uitwisselen, doen dit op een eigen infrastructuur met gegarandeerde performance en beschikbaarheid (goedbeheerd ZorgNetwerk (GZN)). Beheer is ingericht door middel van aangewezen GZN-beheerpartijen met een overkoepelende ketenregie.

Zorgaanbieders die gebruik maken van Nuts-nodes, zijn op het Internet aangesloten om gegevens onderling uit te wisselen, met mogelijk geen performance en beschikbaarheid garanties (afhankelijk van het contract met de desbetreffende Internetprovider).
Elke zorgaanbieder moet zelf het beheer (laten) uitvoeren en bij een probleem in de keten is er (mogelijk) geen regievoering.

5.1.7 Beveiliging

Medische gegevens zijn bijzondere persoonsgegevens. Daarom moet de bescherming van deze gegevens aan de hoogste beveiligingseisen voldoen. Dit geldt zowel voor het XIS als voor de gebruikte infrastructuur. Leidend voor de beveiliging zijn de wetgeving en normen waar alle onderdelen in de keten van gegevensuitwisseling aan moeten voldoen.

Voor AORTA/LSP geldt dat het een eigen infrastructuur betreft zonder directe blootstelling aan het Internet, waardoor de kans op een (directe) hack klein is.
Alle verbindingen binnen deze infrastructuur worden beveiligd met PKI-certificaten en de verbindingen worden opgezet met tweezijdige TLS-authenticatie.
Daarnaast is de infrastructuur ingericht volgens de NEN7510 normen en wordt hier ook jaarlijks op geaudit. Ook wordt er voldaan aan de NEN7512 en 7513 normen voor gegevensuitwisseling en logging.

Zorgaanbieders die gebruik maken van Nuts-nodes, zijn op het Internet aangesloten en hebben directe blootstelling aan het Internet, waardoor de kans om (direct) gehackt te worden groter is.
Alle verbindingen naar Nuts-nodes worden beveiligd met PKI-certificaten.
Daarnaast moeten zorgaanbieders wettelijk voldoen aan de NEN7510 normen en dit moet jaarlijks geaudit worden. Ook moet er voldaan worden aan de NEN7512 en 7513 normen voor gegevensuitwisseling en logging. Onbekend is of de Nuts-nodes aan de NEN-normen voldoen. Er is geen overkoepelend afsprakenstelsel dat dit afdwingt en controleert.

6 Nuts x AORTA/LSP – SOLL

Leeswijzer hoofdstuk

6.1 Gewenste situatie

De meeste zorgaanbieders hebben geen kennis van de verschillende systemen en infrastructuren. Zorgaanbieders willen wel gegevens van hun patiënt kunnen raadplegen wanneer dit nodig is ongeacht waar deze gegevens zich bevinden. Dit betekent dat het mogelijk moet zijn om de op zichzelf staande systemen en infrastructuren met een overkoepelende infrastructuur te verbinden, zodat het mogelijk wordt om gegevens uit te wisselen ongeacht het systeem of infrastructuur dat wordt gebruikt.

6.1.1 Use case

Hiervoor is de onderstaande use case als volgt gedefinieerd:

> *"**Als** raadplegende zorgaanbieder (RPZA), die niet op dezelfde infrastructuur is aangesloten als de dossierhoudende zorgaanbieder (DHZA),*
> ***wil** ik dat een DHZA (aangesloten op een andere infrastructuur dan de RPZA) gegevens van mijn patiënt beschikbaar stelt aan mij,*
> ***zodat** ik mijn patiënt beter kan diagnosticeren en/of behandelen."*
>
> *Volgens de WGBO is de taak van de zorgverlener om **actief, volledig en systematisch** alle medische informatie te verzamelen die noodzakelijk is om tot een verantwoorde diagnose te komen, en deze informatie onverwijld vast te leggen in een beveiligd dossier.*

Deze hoogover use case dekt de specifieke use cases van VVT-zorgaanbieders en zorgaanbieders die aangesloten zijn op het LSP die als volgt zijn opgesteld:

- Use case 1 – Raadplegen actueel medicatieoverzicht
  Als medicatie-toediener in de VVT en als huisarts of andere voorschrijver wil ik kunnen beschikken over één actueel en volledig medicatieoverzicht van de cliënt / patiënt, inclusief recente voorschriften, verstrekkingen, wijzigingen en relevante toedieninformatie, zodat ik veilige beslissingen kan nemen, de juiste medicatie in de juiste dosering op het juiste moment kan voorschrijven of toedienen en medicatiefouten, interacties en doublures worden voorkomen.
- Use case 2 – Inzicht in nieuwe voorschriften, wijzigingen en stoporders
  Als medicatie-toediener in de VVT en als huisarts of andere voorschrijver wil ik direct inzicht hebben in nieuwe voorschriften, doseerwijzigingen, stoporders en tijdelijke aanpassingen, zodat iedereen met dezelfde actuele informatie werkt, verouderde toedienlijsten of voorschriften worden voorkomen en veilig kan worden gehandeld bij wijzigingen in het behandelbeleid.
- Use case 3 – Digitale toedienregistratie en terugkoppeling
  Als medicatie-toediener in de VVT wil ik mijn toedieningen digitaal kunnen registreren en bijzonderheden kunnen terugmelden, en als huisarts of andere voorschrijver wil ik deze terugkoppeling kunnen inzien, zodat afwijkingen, bijwerkingen of therapie-ontrouw tijdig worden gesignaleerd en het behandelplan waar nodig kan worden aangepast.
- Use case 4 – Controle en verificatie bij overdracht of overgang
  Als medicatie-toediener in de VVT en als huisarts of andere voorschrijver wil ik bij opname, ontslag of wijziging van zorgsetting kunnen controleren of het medicatieoverzicht en de voorschriften overeenkomen met de feitelijke situatie van de cliënt / patiënt, zodat overdrachtsfouten worden voorkomen en de continuïteit en veiligheid van farmacotherapie gewaarborgd blijven.

- Use case 5 – Gezamenlijke verantwoordelijkheid en regie
  Als medicatie-toediener in de VVT en als huisarts of andere voorschrijver wil ik duidelijkheid over wie verantwoordelijk is voor welke medicatie-informatie en -actie, inclusief vastlegging van wijzigingen en autorisaties, zodat er geen onduidelijkheid ontstaat over eigenaarschap, aansprakelijkheid en regie binnen de keten.

Specifieke invulling van deze use cases is de wens van VVT-zorgaanbieders en zorgaanbieders die aangesloten zijn op het LSP om medicatiegegevens met elkaar uit te wisselen. Dit wordt verder uitgewerkt in dit document en kan als blauwdruk dienen voor de landelijk infrastructuur en het bijbehorende afsprakenstelsel.

6.1.2 Wet- & regelgeving

Ongeacht of de zorgaanbieders op dezelfde infrastructuur of op verschillende infrastructuren zijn aangesloten, moeten de opslag van medische gegevens en de gegevensuitwisselingen voldoen aan dezelfde wet- en regelgeving zoals beschreven in paragraaf 5.1.1.

6.1.3 Organisatie

Medische gegevens zijn bijzondere persoonsgegevens waaraan de hoogste privacy – en beveiligingseisen worden gesteld voor opslag, toegang en uitwisseling van deze gegevens. Om dit te borgen, naast een zo hoog mogelijke kwaliteit en continuïteit, moeten naast (technische) eisen ook gezamenlijke afspraken, processen en procedures worden gemaakt. Alle betrokken partijen in deze keten die gebruik maken van deze overkoepelende infrastructuur, moeten aan deze(lfde) afspraken en eisen voldoen voordat gegevensuitwisseling kan plaatsvinden. Aangezien het gaat over zorgaanbieders die op verschillende systemen en/of infrastructuren zijn aangesloten, is een landelijke infrastructuur en afsprakenstelsel benodigd.

Voor een landelijke infrastructuur en afsprakenstelsel zijn gezamenlijke eisen, afspraken, processen en procedures benodigd, waarbij de onderstaande punten in ieder geval terug moeten komen:

- Identificatie
  De identificatie van organisaties en personen en welke attributen hiervoor benodigd zijn moet voor alle partijen op dezelfde manier worden ingevuld. De meeste onderwerpen zullen door wetgeving worden ingevuld en waar dit ontbreekt, moeten deze onderwerpen in het afsprakenstelsel en architectuur worden uitgewerkt.
  Voor het identificeren van:
  - een cliënt / patiënt moet het BSN worden gebruikt;
  - een zorgaanbieder moet het URA-nummer worden gebruikt;
  - een BIG-geregistreerde zorgverlener moet het UZI-nummer worden gebruikt;
  - voor een niet-BIG-geregistreerde zorgverlener moet een uniek nummer worden gebruikt;
  - en voor het XIS moet een uniek systeem identificatie worden gebruikt.
- Authenticatie: bij gegevensuitwisseling zijn afspraken nodig op basis waarvan authenticatie van personen en organisaties plaatsvindt. Het type uit te wisselen gegevens bepaalt de eisen die aan de betrouwbaarheid van het authenticatiemiddel wordt gesteld (leidend hierin is eIDAS). Voor de uitwisseling van medische gegevens schrijft de wet voor dat authenticatie op niveau Hoog moet plaatsvinden.
  Voor de authenticatie van VVT-gegevensuitwisselingen worden de volgende authenticatiemiddelen gebruikt:
  - voor een cliënt / patiënt wordt een WID-document gebruikt;
  - voor een zorgaanbieder wordt een geldig UZI-servercertificaat gebruikt;
  - voor een BIG-geregistreerde zorgverlener wordt een geldige UZI-zorgverlenerpas gebruikt;
  - voor een niet-BIG-geregistreerde zorgverlener wordt, bij voorkeur, een UZI-medewerkerspas-op-naam gebruikt of een uniek nummer die komt uit een administratie van de zorgaanbieder, bij voorkeur uit het XIS.
    Dit unieke nummer uit een administratie is geldig nadat een geldige WID-controle heeft plaatsgevonden in de personeelsadministratie;

    - en voor een GTK / GBC moet een getekend (digitaal) contract met de zorgaanbieder aanwezig zijn en het component moet gekwalificeerd zijn.
- Autorisatie: voor uitwisselingen tussen zorgaanbieders moeten autorisatieafspraken worden gemaakt. Hiervoor is een autorisatierichtlijn Medicatieveiligheid opgesteld, inclusief een addendum specifiek voor de VVT en GGZ (20231113__Autorisatierichtlijn Medicatieveiligheid_v1.2_DEF en Addendum_AR_Medicatieveiligheid).
  Voor een niet-BIG-geregistreerde zorgverlener moet een specifieke afgesproken code (taakcode) worden gebruikt zoals in het addendum is gedefinieerd (rolcode 86.000 Verzorgende in de individuele gezondheidszorg).
  Deze rolcode is alleen bruikbaar voor de PoC- en pilotfase. Voor de opschalingsfase moeten hier definitieve afspraken voor gemaakt worden.
  Voor de autorisatie van VVT-gegevensuitwisselingen worden de volgende Verifiable Credentials (VC's) gebruikt:
    - voor een cliënt / patiënt wordt een VC gebruikt die komt uit het XIS, met als voorwaarde dat een geldige WID-controle heeft plaatsgevonden;
    - voor een zorgaanbieder wordt een VC gebruikt waarvoor een geldig UZI-servercertificaat wordt gebruikt;
    - voor een BIG-geregistreerde zorgverlener wordt een VC gebruikt waarvoor een geldige UZI-zorgverlenerpas worden gebruikt;
    - voor een niet-BIG-geregistreerde zorgverlener wordt een VC gebruikt die komt uit de UZI-medewerkerpas-op-naam of uit een administratie van de zorgaanbieder, bij voorkeur uit het XIS. Dit is een uniek nummer binnen de zorgaanbieder en is geldig nadat een geldige WID-controle heeft plaatsgevonden.
- Behandelrelatie: zorgaanbieders zijn verantwoordelijk voor dossierbeheer en goede uitwisseling (NEN75xx) en zorgverleners zijn inhoudelijk verantwoordelijk. Een zorgverlener mag alleen toegang hebben tot (medische) gegevens, wanneer deze een behandelrelatie met de patiënt heeft.
  Aangetoond moet worden dat alleen zorgverlener/zorgmedewerkers die betrokken zijn bij de behandeling van een cliënt / patiënt toegang hebben tot het dossier.
  Dit moet conform NEN7513 worden gelogd en via een eigen verklaring worden aangetoond dat hieraan voldaan wordt.
  Voor de VVT-branche is dit extra belangrijk omdat hier medewerkers werken die niet onder het mandaat van een BIG-geregistreerde zorgverlener werken en wel toegang hebben tot medische persoonsgegevens.
- Patiënttoestemming: bij elektronische uitwisseling van medische gegevens geldt dat de cliënt / patiënt toestemming moet geven voor het beschikbaar stellen van zijn gegevens.
  Vanuit de patiënt gezien moeten zorgaanbieders die op verschillende infrastructuren aangesloten zijn, gebruik maken van hetzelfde toestemmingsregister, zodat de patiënt maar één keer toestemming hoeft te geven.
  Landelijk is de online-toestemmingsvoorziening Mitz hiervoor aangewezen.
- Logging: logging maakt het mogelijk het beheer van uitwisselingen goed in te richten. Wettelijk gezien moet deze logging voldoen aan de NEN7513 en via een eigen verklaring worden aangetoond dat hieraan voldaan wordt.
  In de AORTA-architectuur zijn hier reeds eisen voor opgesteld voor de gehele keten. Voor VVT-instellingen is er geen overkoepelende keten en moet dit voor elke schakel in de keten worden gecontroleerd c.q. afspraken over worden gemaakt.
- Transparantie: transparantie omvat afspraken over hoe zorgaanbieders, zorgverleners en patiënten kunnen weten wat de afspraken over de waarborgen in het vertrouwensmodel zijn. Zorgverleners moeten op de hoogte zijn van het beleid op de waarborgen van het vertrouwensmodel, zowel intern als bij uitwisseling tussen zorgaanbieders. Voordat een zorgaanbieder uitwisselt met andere zorgaanbieders, moet deze op de hoogte zijn van de vastgelegde afspraken hierover. De zorgaanbieder zal, net als de andere deelnemende zorgaanbieders, aan de afspraken moeten voldoen.
  Voor uitwisselingen op het LSP wordt dit inzichtelijk gemaakt door in te loggen op VolgJeZorg.nl. Uitwisselingen met VVT-instellingen en LSP-deelnemers worden hier ook getoond.

- Lokalisatie: het lokaliseren van andere dossierhoudende zorgaanbieders wordt aangemerkt als bijzondere persoonsgegevens waarvoor toestemming van de cliënt / patiënt is vereist. Alleen als de cliënt / patiënt toestemming heeft gegeven voor een specifieke dossierhouder, wordt de desbetreffende dossierhoudende zorgaanbieder als bron doorgegeven. Zorgaanbieders die op verschillende infrastructuren aangesloten zijn, moeten gebruik maken van hetzelfde lokalisatieregister, anders is het mogelijk dat niet alle dossierhoudende zorgaanbieders worden gevonden (waar de cliënt / patiënt toestemming voor heeft gegeven).
  In de PoC- en pilotfase wordt er niet gelokaliseerd door een GTK. In de opschalingsfase moet er wel gelokaliseerd kunnen worden en moet een keuze gemaakt worden voor een lokalisatieregister.
- Adressering: adressering is zowel noodzakelijk bij het ongericht beschikbaar stellen als bij het gericht versturen van informatie. De communicatieknooppunten moeten weten achter welk communicatieknooppunt een gewenste dossierhoudende zorgaanbieder zit. Ook kan via adressering informatie, bijvoorbeeld technische endpoints of zorgaanbiedertype, over een zorgaanbieder worden opgevraagd.
  Voor zowel lokalisatie als voor toestemming is het zorgaanbiedertype benodigd. Deze kan aan de hand van het URA-nummer uit het ZORG-AB worden gehaald.
  Daarnaast maakt een GTK van het ZORG-AB gebruik om via de URA het technische endpoint op te halen voor de door de zorgaanbieder gebruikte GTK.
- Verantwoordelijkheden leveranciers: deze moeten worden bepaald en opgesteld, zodat deze afspraken over SLA's, processen, procedures, beveiliging en naleving van wettelijke verplichtingen worden vastgelegd en geïmplementeerd.
- Audit en compliance: ditzelfde geldt voor interne controles, incidentmeldingen en documentatie voor toezichthouders (IGJ, AP).

Twiin ontwikkelt zelf geen afsprakenstelsel, maar heeft een overkoepelend afsprakenstelsel die ervoor zorgt dat bestaande afsprakenstelsels op elkaar afgestemd zijn, zodat er voldoende vertrouwen bestaat dat gegevensuitwisselingen tussen infrastructuren voldoet aan (min of meer) dezelfde eisen van de onderwerpen die hierboven zijn benoemd.

Momenteel staan de VVT-instellingen op zichzelf en wisselen zelfstandig gegevens uit op onderlinge afspraken. Dit is niet houdbaar voor gegevensuitwisselingen tussen verschillende infrastructuren, het is ondoenlijk om op individuele basis met elke zorgaanbieder afspraken te maken over deze gegevensuitwisselingen. Voor deze gegevensuitwisselingen dienen de VVT-instellingen te voldoen aan de eisen die de desbetreffende infrastructuur aan de gegevensuitwisselingen stellen.
Dit betekent dat voor de opschalingsfase de organisaties in de VVT-instellingenketen een eigen afsprakenstelsel moeten hebben die gelijkwaardige afspraken en architectuur bevatten. Een andere optie is dat deze organisaties deelnemer worden in het AORTA-afsprakenstelsel waarin deze afspraken en architectuur als zijn vastgelegd.

Specifiek voor de gegevensuitwisseling van medicatiegegevens tussen VVT-instellingen en huisartsen zijn alleen voor de PoC- en pilotfase afspraken gemaakt met de huisartsenkoepels. Voor de opschalingsfase moeten de definitieve afspraken gemaakt worden op welke basis deze gegevensuitwisselingen plaats mogen vinden.

6.1.4 Zorgproces

Door gebruik te maken van gemeenschappelijke voorzieningen (implementatie van generieke functies) wordt meer en meer een uniforme wijze van adressering, lokalisatie, verwijsindex, logging, mogelijk. Hierdoor 'merkt' het zorgproces feitelijk niet dat er een overgang wordt gemaakt over de verschillende afsprakenstelsels heen. De systemen ondersteunen de verschillende technische implementaties via gestandaardiseerde knooppunten en andere ondersteunende software binnen het eigen platform.

Om het zorgproces te optimaliseren zijn vaak gegevens van andere zorgaanbieders benodigd. In het geval van de VVT gaat het specifiek om medicatiegegevens.

Voor het opvragen van de medicatiegegevens is de patiënttoestemming vereist. Elke zorgaanbieder dient daarom een proces ingericht te hebben om de cliënt / patiënt hierover voor te lichten, zodat de cliënt /

patiënt goed geïnformeerd en uit vrije wil deze toestemmingen in Mitz kan vastleggen, zodat er, afhankelijk of er wel of geen toestemming is verleend, daadwerkelijk gegevens uitgewisseld kunnen worden. Deze toestemming wordt gecontroleerd door de specifieke componenten in de keten van gegevensuitwisseling voor het lokaliseren en het beschikbaar stellen van gegevens.

Voor BIG-geregistreerde zorgverleners moet bepaald worden welke rolcodes welke gegevens mogen ontvangen. Daarnaast moet voor een niet-BIG-geregistreerde zorgverlener een taakcode toegewezen krijgen, waarbij de juiste medicatiegegevens opgevraagd kunnen worden. Dit allemaal conform de definitieve autorisatierichtlijn die nog afgestemd moet worden.

De zorgverlener die medicatie toedient is verantwoordelijk voor de registratie hiervan in het desbetreffende dossier. Hierdoor wordt het mogelijk dat de voorschrijvende zorgverlener op de hoogte is dat de cliënt / patiënt wel of niet de daadwerkelijk voorgeschreven medicatie heeft ingenomen.

6.1.5 Informatie

De informatie die uitgewisseld wordt is in het programma Medicatieoverdracht uitgewerkt. Deze maakt gebruik van onder andere de informatiestandaarden MP9, ZIB en FHIR. De zorgaanbieders dienen deze informatiestandaarden binnen hun ECD's / EPD's en infrastructuur dan ook te ondersteunen.

Voor de taakcodes dient een codetabel opgesteld te worden zodat de juiste gegevens volgens de definitieve autorisatierichtlijn uitgewisseld kunnen worden.

6.1.6 Applicatie

Het XIS moet alle (informatie)standaarden en formaten, die bij deze gegevensuitwisselingen behoren, ondersteunen. Daarnaast moet het XIS de functionaliteiten hebben om op de desbetreffende infrastructuur te kunnen communiceren.

Het moet mogelijk zijn om voor niet-BIG-geregistreerde zorgverleners een taakcode te definiëren.

6.1.7 Infrastructuur & beveiliging

Om de gewenste gegevensuitwisseling te kunnen ondersteunen en de veiligheid te kunnen borgen, moet binnen de infrastructuur ondersteuning zijn voor de toegestane authenticatiemiddelen (UZI, eIDAS hoog middelen, andere authenticatiemiddelen) in combinatie met (toekomstige) DEZI en de waarborgen (VC's en SAML2) en het beheer hiervan (onder andere controle geldigheid en het intrekken van authenticatiemiddelen).

De beveiliging van de infrastructuur moet minimaal conform de wet- en regelgeving en de actuele industriestandaarden zijn. De verbindingen tussen de ketenpartners moeten worden opgezet via tweezijdige TLS-verbindingen (met de TLS-classificatie goed).

In de keten dienen afspraken gemaakt te worden over de performance en beschikbaarheid in de gehele keten.

Ook moeten in de keten afspraken gemaakt worden over de monitoring van de verschillende componenten in de communicatieketen van de gegevensuitwisseling.

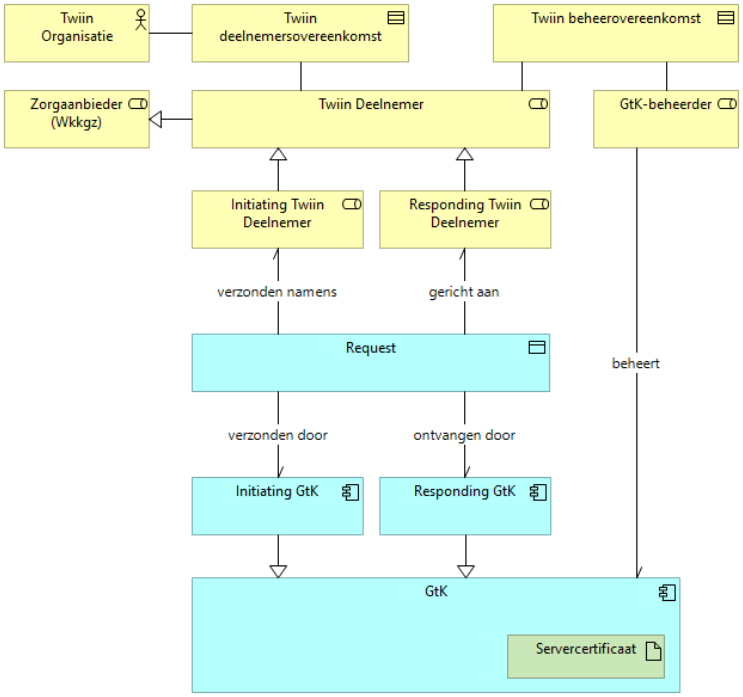
6.2 Toekomstige situatie

Om verschillende infrastructuren met elkaar te kunnen laten communiceren, zoals Nuts en AORTA/LSP, is een overkoepelend afsprakenstelsel benodigd en Twiin is dan de logische keuze. Twiin biedt zelf geen netwerk en diensten, maar een raamwerk waarbinnen zelfstandige infrastructuren verbonden kunnen worden om te kunnen samenwerken.

Twiin specificeert verplichte architecturale patronen (zoals het gebruik van GtK's), toepasselijke standaarden (zoals FHIR), vertrouwens- en autorisatieprincipes en de scheiding van verantwoordelijkheden tussen deelnemende domeinen.

Om gebruik te kunnen maken van Twiin, dient de zorgaanbieder een Twiin-deelnemersovereenkomst te sluiten met de Twiin-organisatie. Daarnaast dient de zorgaanbieder een Twiin-beheerovereenkomst te

sluiten met een GtK-beheerorganisatie, waarin wordt beschreven op welke wijze de GtK-beheerder de GtK van de Twiin-deelnemer beheert.



Om vertrouwen te creëren tussen de initiërende 'Twiin Deelnemer' en de reagerende 'Twiin Deelnemer', moet aan de volgende vereisten worden voldaan.

Wanneer een initiërende GtK een verzoek wil verzenden, moet deze kunnen vaststellen:

1. dat de ontvangende organisatie een zorginstelling is;
2. dat de ontvangende organisatie een 'Twiin Deelnemer' is;
3. welke 'GtK-beheerder' en GtK door de reagerende 'Twiin Deelnemer' gemachtigd zijn om het verzoek te verwerken;
4. dat het ontvangende systeem daadwerkelijk de beoogde GtK is (endpoint authenticiteit);
5. dat de reagerende GtK en 'GtK-beheerder' door 'Twiin' gekwalificeerd zijn om dit specifieke type verzoek te ontvangen;
6. dat de beveiligde verbinding met de reagerende GtK tot stand is gebracht (bijv. TLS).

Wanneer een GtK die reageert een verzoek ontvangt, moet deze het volgende kunnen vaststellen:

1. van welk systeem het verzoek afkomstig is en dat het verzendende systeem een GtK is (systeemauthenticiteit);
2. welke 'GtK-beheerder' de initiërende GtK beheert;
3. dat de initiërende GtK en de 'GtK-beheerder' door Twiin zijn gekwalificeerd om dit type verzoek te verzenden;
4. namens welke organisatie het verzoek wordt verzonden en dat deze organisatie een zorginstelling en een 'Twiin-deelnemer' is;
5. dat de initiërende 'Twiin-deelnemer' de 'GtK-beheerder' en de initiërende GtK machtigt om namens hem/haar te handelen;
6. dat de integriteit van het verzoek is gegarandeerd (bijv. digitale handtekening).

Daarnaast moet de GtK-beheerorganisatie ook een Twiin-overeenkomst ondertekenen. De door de GtK-beheerorganisatie ontwikkelde GtK moet gekwalificeerd worden door Twiin voordat deze in productie mag worden genomen.

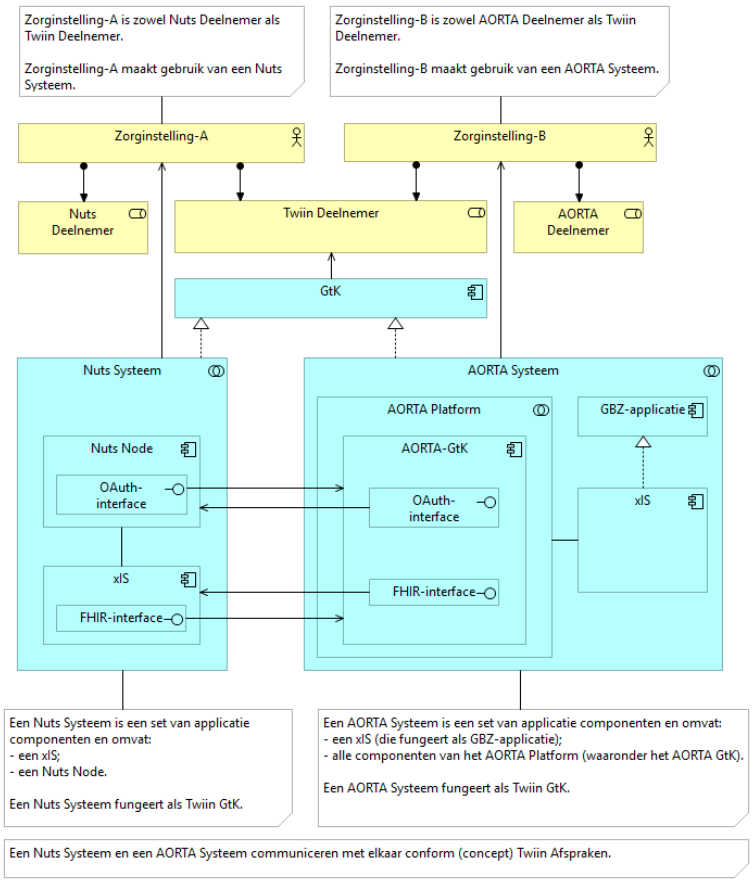
Om veilige, interoperabele en aan de regelgeving conforme communicatie tussen infrastructuren te waarborgen, worden alle interacties tussen de Nuts- en AORTA/LSP via een GtK (Gevalideerd Twiin Knooppunt) geleid. Het GtK fungeert als een gecontroleerde vertrouwensgrens die de interne identiteits-, autorisatie- en protocolmodellen van elk ecosysteem loskoppelt van externe afnemers en aanbieders van zorggegevens.

Het GtK vertegenwoordigt het beoogde convergentiepunt voor gevalideerd domeinoverschrijdend vertrouwen. Formele validatie van het GtK-concept kan pas plaatsvinden nadat deze specificaties zijn geïmplementeerd en beoordeeld binnen het Twiin-raamwerk. Tot die tijd verwijzen verwijzingen naar het GtK naar de infrastructurele en architecturale component, zonder dat dit een formele Twiin-kwalificatie impliceert. Tijdens de PoC- en Pilot-fase wordt de vertrouwensbasis gedefinieerd binnen het AORTA-raamwerk.

Er is een Twiin-deelnemersovereenkomst gesloten tussen een Twiin-deelnemer (zorgverlener of zorginstelling) en de Twiin-organisatie. Er is een Twiin-beheerovereenkomst gesloten tussen een Twiin-deelnemer en zijn GtK-beheerder (organisatie), waarin de wijze waarop de GtK-beheerder de GtK van de Twiin-deelnemer beheert, wordt beschreven.

In de Twiin GtK-architectuur wordt een identiteit niet langer bevestigd door de transportlaag, maar aangetoond door cryptografisch bezit van referenties die zijn uitgegeven onder een gezaghebbend vertrouwenskader.

Voor de PoC- en Pilot-fase zijn deze overeenkomsten nog niet benodigd. Momenteel is er geen programma van eisen (PvE) en implementatiehandleiding (IH) voor een GtK en Twiin zal deze ook niet zelf opstellen. Daarom zal uit de specificaties in dit document een PvE en IH Goed Beheerde Connector (GBC) worden opgesteld waarin de randvoorwaarden voor een GtK uit het Twiin-afsprakenstelsel ook zijn opgenomen. Deze PvE en IH GBC zal dan worden ingebracht in het Twiin-afsprakenstelsel als PvE en IH GtK.



7 Requirements & onderzoeksvragen

7.1 Inleiding

Dit hoofdstuk beschrijft de requirements en onderzoeksvragen voor de harmonisatie van de vertrouwensmodellen van het Nuts-netwerk en de AORTA-infrastructuur van VZVZ. Het doel is om tot een gedeeld authenticatie- en identificatieframework te komen waarbinnen beide infrastructuren kunnen samenwerken, zonder dat de bestaande werking van het LSP of het Nuts-netwerk fundamenteel wordt aangetast.

De requirements zijn opgebouwd van generiek naar specifiek. We beginnen met overkoepelende harmonisatie-eisen die gelden ongeacht de gekozen technische oplossing. Vervolgens worden generieke eisen voor lokalisatie, identificatie, authenticatie en adressering beschreven. Voor lokalisatie en adressering stellen we hoog over eisen op en verwijzen we grotendeels naar bestaande uitwerkingen. Identificatie en authenticatie vormen de kern van dit hoofdstuk, omdat de vertrouwensmodellen van beide infrastructuren hier op elkaar gelegd moeten worden.

Het hoofdstuk sluit af met een overzicht van open onderzoeksvragen en designkeuzes waar de requirements nog niet eenduidig zijn. Bij elke onderzoeksvraag wordt beschreven welke impact de mogelijke keuzes hebben op de oplossing als geheel.

7.2 Uitgangspunten en scope

7.2.1 Scope

Dit hoofdstuk behandelt de VWS Generieke Functies lokalisatie, identificatie, authenticatie en adressering. Autorisatie en toestemming vallen buiten scope. Voor lokalisatie en adressering zijn reeds uitwerkingen beschikbaar, dit hoofdstuk stelt alleen generieke eisen relevant voor de harmonisatie. Identificatie en authenticatie vormen de kern van dit hoofdstuk.

De oplossing moet passen binnen het wettelijk kader; WGBO, AVG, WABVPZ, waarbij de dienstverlener in ‘opdracht’ werkt van de zorgaanbieder. Omdat een dienstverlener nooit een zelfstandige verwerker, maar altijd een subverwerker van een zorgaanbieder zullen de bevoegdheden traceable en auditable moeten zijn vanuit de verantwoordelijkheden van de zorgaanbieder.

Het concept ‘delegatie’ wordt in dit document besproken voor de inrichting van een Gtk, maar deze delegaties kunnen ook plaats gaan vinden in andere contexten (aanvullende diensten, DSS, vertalingen, externe (sub)functies van zorgsystemen, etc..).

7.2.2 Stip op de horizon

De ambitie is een geharmoniseerd vertrouwensmodel waarin:

- Alle deelnemende partijen identificeerbaar en authenticeerbaar zijn ongeacht het netwerk waaruit ze afkomstig zijn
- Deelname mogelijk is op basis van alle in Nederland toegelaten authenticatiemiddelen voor de gezondheidszorg.
- Nieuwe partijen en netwerken kunnen toetreden zonder dat bestaande deelnemers aanpassingen hoeven te doen

7.2.3 Huidig vertrekpunt

Niet alle ambities zijn op dit moment realiseerbaar. De requirements maken daarom onderscheid tussen wat nu haalbaar is (MOET) en wat op termijn gewenst is (ZOU MOETEN). Dit initiatief opereert binnen de bredere landelijke transitie van afsprakenstelsels. Hoewel het een geïsoleerd initiatief betreft, zoekt het aansluiting bij landelijke ontwikkelingen en streeft het ernaar als koploper richting te geven.

7.3 Eisen aan de Harmonisatie

Overkoepelend (interoperabiliteit, backward compatibility, governance)

ID	Requirement	Rationale
1	De huidige Nuts- en LSP-toepassingen MOETEN ongestoord blijven functioneren tijdens en na de harmonisatie	Continuïteit van zorg mag niet in gevaar komen door infrastructuurwijzigingen
2	Bestaande autorisatierichtlijnen en het huidige trust framework MOETEN ongewijzigd blijven	De harmonisatie richt zich op de authenticatielaag, niet op het aanpassen van bestaande autorisatieafspraken
3	Nuts-nodes MOETEN als zelfstandig (Twiin-)knooppunt functioneren, waarmee het Nuts-netwerk decentraal wordt ontsloten	Het decentrale karakter van het Nuts-netwerk moet behouden blijven binnen de geharmoniseerde infrastructuur
4	De geharmoniseerde afspraken MOETEN passen binnen het landelijke GIS en opneembaar zijn in afsprakenstelsels zoals Twiin	Het doel is een landelijke infrastructuur, niet een 1-op-1 koppeling
5	De oplossing ZOU bruikbaar MOETEN zijn zonder dat zorgmedewerkers (met name in de VVT-sector) verplicht een UZI-pas nodig hebben	Veel Nuts-partijen in de VVT beschikken momenteel niet over UZI-passen. Dit is op dit moment nog niet mogelijk, maar is een wens om adoptie niet te blokkeren
6	Partijen MOETEN gefaseerd kunnen aansluiten zonder dat alle deelnemers gelijktijdig moeten overstappen	Een gelijktijdige overgang is niet realistisch bij landelijke schaal met diverse partijen
7	De implementatiedrempel voor toetreding ZOU minimaal MOETEN zijn, met name voor kleinere organisaties en leveranciers	De VVT- en eerstelijnssector kennen veel kleinere organisaties met beperkte IT-capaciteit
8	De oplossing MOET geen vendor lock-in creëren en open standaarden gebruiken	Interoperabiliteit en keuzevrijheid zijn kernprincipes van zowel Nuts als het bredere Twiin-stelsel
9	Het LSP MOET LSP-deelnemers transparant via een (Twiin-)knooppunt toegang bieden tot het landelijk netwerk, zonder dat deelnemers hiervan kennis hoeven te hebben of aanpassingen hoeven te doen	Transparantie voor achterliggende partijen verlaagt de adoptiedrempel en voorkomt dat de harmonisatie doorwerkt in bestaande implementaties
10	Deelnemers aan het ene netwerk ZOUDEN NIET verplicht MOETEN worden een (verwerkers)overeenkomst aan te gaan met een knooppunt of infrastructuurpartij van het andere netwerk om gegevens te kunnen uitwisselen	Partijen moeten kunnen deelnemen aan gegevensuitwisseling zonder juridische afhankelijkheid van infrastructuurpartijen waarmee zij geen directe relatie hebben
11	De oplossing ZOU zoveel mogelijk gebruik MOETEN maken van de landelijke generieke functies.	VWS ontwikkelt samen met het veld generieke functies voor vertrouwen. Deze zijn echter nog in ontwikkeling en niet allemaal al beschikbaar. Een eventuele tijdelijke oplossing probeert zoveel mogelijk in lijn met deze landelijke ontwikkelingen te zijn.
12	De oplossing MOET voorzien in een versioneringsvoorziening zodat na invoering claims kunnen worden gewijzigd dan wel uitgebreid	Infrastructuren ontwikkelen zich, ook het LDN, Twiin, AORTA en Nuts. Sommige ontwikkelingen vereisen infrastructurele wijzigingen. De bestaande claims mogen niet belemmerend zijn voor doorontwikkeling, Wel zouden nieuwe versies vereist kunnen worden.

7.4 Eisen aan Lokalisatie

De lokalisatiefunctie maakt indien beschikbaar gebruik van de Nationale Verwijs Index (NVI) zoals is beschreven in de Generieke Functies Lokalisatie specificatie (nog in ontwikkeling). De NVI stelt zorgverleners in staat om te ontdekken welke organisaties relevante patiëntgegevens van een bepaald type beschikbaar hebben. Onderstaande requirements beschrijven de eisen die richtinggevend zijn voor de harmonisatie van deze lokalisatiefunctie.

ID	Requirement	Rationale
LOK-01	Zowel partijen aangesloten via het LSP als via het Nuts-netwerk MOETEN lokalisatierecords kunnen registreren bij de NVI	Beide netwerken moeten gelijkwaardig kunnen deelnemen aan de nationale verwijsindex
LOK-02	Zowel partijen aangesloten via het LSP als via het Nuts-netwerk MOETEN de NVI kunnen bevragen, op een geautoriseerde en auditeerbare wijze, om datahouders voor een specifieke patiënt en gegevenstype te vinden	De lokalisatiefunctie moet netwerk agnostisch bruikbaar zijn
LOK-03	Het LSP MOET lokalisatierecords namens haar achterliggende systemen kunnen registreren en beheren, zonder dat die systemen hier zelf actie voor hoeven te ondernemen	Consistent met HAR-010; het LSP fungeert als knooppunt en abstraheert de complexiteit voor achterliggende partijen
LOK-04	De authenticatie-attributen die de NVI vereist (URA, organisatietype, UZI/DEZI, rolcode) MOETEN afleidbaar zijn uit het geharmoniseerde authenticatiemodel	De NVI stelt eisen aan de identiteit van de bevragende partij, het authenticatiemodel moet deze attributen kunnen leveren, ongeacht het netwerk van herkomst

7.5 Eisen aan Identificatie

7.5.1 Partijen en rollen

Deze sectie beschrijft welke entiteiten deelnemen aan gegevensuitwisseling en aan welke eisen hun identificatie moet voldoen. Het gaat hier om de partijen zelf en de wijze waarop zij eenduidig herkenbaar zijn binnen het geharmoniseerde model. De relaties tussen deze partijen worden behandeld in sectie 7.5.2 en 7.5.3.

ID	Requirement	Rationale
IDENT-001	Zorgaanbieders MOETEN uniek identificeerbaar zijn aan de hand van het URA-nummer, uitgegeven door het CIBG (UZI-register)	Het URA-nummer is de landelijk erkende identifier voor zorgaanbieders
IDENT-002	Niet-zorgaanbieders (zoals dienstverleners en softwareleveranciers) MOETEN identificeerbaar zijn aan de hand van het KVK-nummer “waarbij aanvullende identificatie nodig kan zijn voor specifieke diensten of technische componenten	Dienstverleners zijn niet geregistreerd in zorgspecifieke registers; het Handelsregister is de autoritatieve bron
IDENT-003	Zorgverleners MOETEN uniek identificeerbaar zijn aan de hand van het UZI/DEZI-nummer, uitgegeven door het CIBG	Het UZI/DEZI-nummer is de landelijk erkende identifier voor zorgprofessionals
IDENT-004	Patiënten MOETEN uniek identificeerbaar zijn aan de hand van	Het BSN is de wettelijk verplichte identifier voor patiënten in de Nederlandse zorg

	het BSN, met de BRP als autoritatieve bron	
IDENT-005	Zorgaanbieders MOETEN classificeerbaar zijn op basis van organisatietype aan de hand van een gestandaardiseerd classificatiesysteem	Verschillende toepassingen vereisen kennis van het type organisatie (ziekenhuis, huisartsenpraktijk, apotheek, etc.) voor beleids- en autorisatiebeslissingen
IDENT-006	Sub-organisatorische eenheden (afdelingen, locaties, zorgdiensten) MOETEN identificeerbaar zijn via lokaal toegekende, binnen de organisatie unieke identifiers , met een aantoonbare relatie tot de bovenliggende organisatie (URA)	Het URA-register dekt geen sub-organisatorische eenheden, maar deze moeten wel herleidbaar zijn tot de verantwoordelijke organisatie
IDENT-007	Elke identiteitsclaim MOET afkomstig zijn van de autoritatieve bron die verantwoordelijk is voor het betreffende attribuut	Elke identiteitseigenschap (professionele kwalificatie, organisatieregistratie, rolbenoeming) heeft een aangewezen autoritatieve bron. Claims van andere partijen kunnen niet vertrouwd worden
IDENT-008	Het identificatieframework MOET pseudonimisering van patiëntidentificatie ondersteunen waar dit vereist is	Privacywetgeving en specifieke toepassingen kunnen vereisen dat het BSN niet direct wordt uitgewisseld
IDENT-009	Het MOET mogelijk zijn om nieuwe typen claims en autoritatieve bronnen toe te voegen zonder wijzigingen aan bestaande infrastructuur of implementaties	De zorgsector ontwikkelt continu nieuwe uitwisselingsscenario's; het model moet uitbreidbaar zijn zonder bestaande partijen te raken
IDENT-0091	Identifiers MOETEN persistent en stabiel zijn over de tijd	Is essentieel voor logging, auditing, herleidbaarheid. En het voorkomt problemen bij migraties.

7.5.2 Verhoudingen tussen partijen

Deze sectie beschrijft de fundamentele relaties tussen de partijen uit sectie 7.5.1. Het gaat hier om de structurele verhoudingen: welke partijen namens welke andere partijen mogen handelen, hoe verantwoordelijkheid is belegd, en welke principes gelden voor het identiteitsmodel als geheel. De concrete eisen aan hoe deze verhoudingen worden ingericht, beheerd en gecontroleerd — met name op het gebied van delegatie — worden uitgewerkt in sectie 7.5.3.

ID	Requirement	Rationale
IDENT-010	Een zorgaanbieder MOET bevoegdheden kunnen toekennen aan een derde partij om namens haar te handelen in het digitale domein	Zorgaanbieders besteden IT-dienstverlening uit aan dienstverleners (EPD-leveranciers, MSP's). Dit moet expliciet gemodelleerd zijn
IDENT-011	Een dienstverlener MOET meerdere zorgaanbieders kunnen bedienen	Dienstverleners opereren doorgaans als multi-tenant; het model moet dit ondersteunen

IDENT-012	Een zorgaanbieder KAN uitsluitend bevoegdheden delegeren die zij zelf bezit	Subdelegatie van bevoegdheden die de zorgaanbieder zelf niet heeft, is niet toegestaan
IDENT-013	Delegatie van handelingsbevoegdheid MAG NIET worden geïnterpreteerd als overdracht van verantwoordelijkheid; de zorgaanbieder blijft verantwoordelijk	De wettelijke en inhoudelijke verantwoordelijkheid blijft bij de zorgaanbieder, ook wanneer een dienstverlener namens haar handelt
IDENT-014	Een claim MOET altijd betrekking hebben op de partij die er het onderwerp van is; de presenterende partij en het onderwerp van de claim MOGEN verschillend zijn	Zonder dit onderscheid is delegatie niet mogelijk. De semantiek moet correct blijven: een claim over een zorgaanbieder blijft een claim over die zorgaanbieder, ook als een dienstverlener deze presenteert
IDENT-0141	Elke gedelegeerde handeling MOET herleidbaar zijn tot zowel de uitvoerende partij als de zorgaanbieder namens wie wordt gehandeld	Essentieel voor **NEN7510 / NEN7513** en sluit aan op logging, auditing, accountability

7.5.3 Delegatie

Sectie 5.2 beschrijft dat partijen namens elkaar kunnen handelen en welke principes daarbij gelden. Deze sectie werkt uit welke eisen gesteld worden aan de delegatie zelf: hoe bevoegdheden worden toegekend en afgebakend, hoe delegaties controleerbaar en intrekbaar zijn, en welke eigenschappen een delegatiebewijs moet hebben. Eisen aan de verificatie en presentatie van delegatiebewijzen — het technische proces van aantonen en controleren — worden behandeld in sectie 6 (Authenticatie).

ID	Requirement	Rationale
IDENT-015	De toegekende bevoegdheden MOETEN duidelijk en expliciet afgebakend zijn	Onbegrensde delegatie creëert onacceptabele risico's. De scope (toepassingen, handelingen, diensten) moet eenduidig zijn
IDENT-016	Een zorgaanbieder MOET meerdere delegaties parallel kunnen afgeven aan verschillende dienstverleners	Zorgaanbieders werken vaak met meerdere leveranciers (EPD, beeldvorming, lab). Elke relatie moet onafhankelijk beheerbaar zijn
IDENT-017	Delegaties MOETEN zowel tijdelijk als structureel kunnen zijn	Sommige relaties zijn projectmatig of tijdelijk; andere zijn langlopend
IDENT-018	Het MOET ondubbelzinnig en **verifieerbaar** vaststelbaar zijn welke dienstverlener namens welke zorgaanbieder handelt	Regelgeving (NEN 7510, AVG/GDPR) vereist herleidbare verantwoordelijkheid. De relatie moet onweerlegbaar zijn
IDENT-019	De zorgaanbieder MOET een delegatie direct kunnen intrekken	Zorgaanbieders moeten de controle behouden over wie namens hen handelt
IDENT-020	Delegaties MOETEN onafhankelijk controleerbaar zijn door derden, zonder tussenkomst van de betrokken partijen op het moment van controle	Een verifiërende partij moet op het moment van een transactie de geldigheid van een delegatie kunnen vaststellen zonder afhankelijk te zijn van de beschikbaarheid van de delegerende of gedelegeerde partij

IDENT-021	Het gebruik van delegaties MOET volledig auditeerbaar zijn, **inclusief wie, wanneer en onder welke delegatie heeft gehandeld**.	Voor compliance en verantwoording moet vastgelegd kunnen worden wanneer en hoe delegaties zijn gebruikt
IDENT-022	Wanneer een partij een claim presenteert over een andere partij, MOET hiervoor een expliciete en verifieerbare autorisatie bestaan	Het presenteren van claims namens een ander zonder aantoonbare toestemming ondermijnt het vertrouwensmodel
IDENT-023	Het delegatiebewijs MOET expliciet vastleggen dat de zorgaanbieder de dienstverlener autoriseert om namens haar te handelen	Impliciete delegatie (bv. via gedeelde certificaten of technische authenticatierelaties) ondermijnt de verantwoording
IDENT-024	Het delegatiebewijs MOET expliciet vastleggen dat de dienstverlener geautoriseerd is om claims over de zorgaanbieder te presenteren	Autorisatie om te handelen en autorisatie om claims te presenteren zijn twee verschillende bevoegdheden die beide expliciet moeten zijn
IDENT-025	Het delegatiemodel MOET onafhankelijke intrekking van delegatiebewijzen ondersteunen	Gecompromitteerde of ingetrokken delegaties moeten beëindigd kunnen worden. De controle hierover ligt bij de zorgaanbieder (zie IDENT-019)
IDENT-026	Dienstverleners MOETEN aantoonbaar zijn toegelaten tot het stelsel waarbinnen zij opereren, op basis van door het stelsel gestelde eisen (bv. certificeringen, kwalificaties)	Alleen gekwalificeerde partijen mogen deelnemen aan gegevensuitwisseling. Toelating is een voorwaarde voor het verkrijgen van delegaties
IDENT-027	Een delegatie MOET cryptografisch of anderszins sterk gebonden zijn aan de identiteit van zowel de zorgaanbieder als de dienstverlener.	Voorkomt “losse” delegaties en sluit aan op VC's en ander werk zoals SAML assertions

7.6 Eisen aan Authenticatie

7.6.1 Generieke authenticatie-eisen

Deze sectie beschrijft de overkoepelende eisen aan het authenticatieproces. Het gaat om functionele en beveiligingseisen die gelden ongeacht de gekozen technische implementatie. Specifieke eisen aan sleutelmateriaal, verificatie van delegatie, wallets, presentatie en het OAuth-profiel worden in de volgende secties behandeld.

ID	Requirement	Rationale
AUTH-001	Het MOET mogelijk zijn om claims van verschillende autoritatieve bronnen te combineren in een enkele transactie	Een interactie kan bewijs vereisen van organisatie-identiteit (URA-register), professionele kwalificatie (UZI-register) en rolbenoeming (werkgever) -- alle van verschillende bronnen
AUTH-002	Een verifiërende partij MOET de volledige vertrouwensketen **cryptografisch** kunnen valideren zonder op het moment van verificatie contact te hoeven maken met de uitgever van de claim	Runtime-afhankelijkheden van externe systemen creëren beschikbaarheids- en prestatierisico's

AUTH-003	Alleen de claims die noodzakelijk zijn voor een specifieke transactie MOGEN gedeeld worden met de verifiërende partij. Dit geldt zowel per transactie als per bronhouder	Privacywetgeving (AVG/GDPR) vereist dataminimalisatie. Een bronhouder mag alleen de claims ontvangen die relevant zijn voor de interactie met die specifieke bronhouder
AUTH-004	Authenticatiestromen MOETEN zowel interacties met als zonder directe betrokkenheid van een eindgebruiker ondersteunen	De zorgsector vereist zowel door zorgverleners geïnitieerde toegang als geautomatiseerde systeem-naar-systeem communicatie (labresultaten, notificaties)
AUTH-005	Authenticatie MOET gebruiksvriendelijk zijn voor zorgverleners; herhaalde authenticatie per transactie MOET vermeden worden	Zorgverleners werken onder tijdsdruk. Herhaalde authenticatie verstoort het werkproces en verlaagt adoptie
AUTH-006	Het authenticatieframework MOET flexibel omgaan met veranderende identificatiemiddelen en -voorzieningen	Er zal altijd een huidige en een volgende generatie identificatiemiddelen naast elkaar bestaan (bv. UZI-passen, servercertificaten, DEZI, DigiD). De oplossing mag niet gekoppeld zijn aan één specifiek middel of voorziening
AUTH-007	Het authenticatieframework MOET meerdere deployment-modellen ondersteunen (geïntegreerde systemen, managed services, cloudoplossingen) zonder wijzigingen aan de specificatie	Organisaties hebben uiteenlopende technische volwassenheid en leveranciersrelaties. De specificatie definieert interoperabiliteit op de grens, niet interne implementatiekeuzes
AUTH-008	Authenticatie tussen twee partijen MAG NIET afhankelijk zijn van de synchrone runtime-beschikbaarheid van derde partijen	Landelijke zorginfrastructuur kan niet afhankelijk zijn van componenten waarvan de uitval authenticatie zou blokkeren
AUTH-0081	Authenticatiebewijzen MOETEN cryptografisch beschermd zijn tegen wijziging en herleidbaar zijn tot de uitgevende partij	Zonder cryptografische integriteit en herleidbaarheid kan de ontvanger niet vaststellen of een bewijs authentiek is of gemanipuleerd. Dit ondermijnt het vertrouwen in de identiteit en de bron van de claims en maakt misbruik mogelijk.
AUTH-0082	Authenticatiebewijzen MOETEN beschermd zijn tegen ongeautoriseerd hergebruik in andere transacties (replay-aanvallen)	Zonder bescherming tegen hergebruik kunnen geldige authenticatiebewijzen worden onderschept en opnieuw gebruikt in een andere context. Dit leidt tot onbevoegde toegang en vormt een direct beveiligingsrisico voor systemen en gegevensuitwisseling.
AUTH-0083	Authenticatiebewijzen MOETEN gebonden kunnen worden aan de context van de transactie (zoals partij, doel of interactie)	Contextbinding voorkomt dat een geldig bewijs buiten de bedoelde context wordt gebruikt. Door het bewijs te koppelen aan specifieke partijen, doelen of interacties wordt misbruik beperkt en wordt de juistheid van de autorisatiebeslissing versterkt.

7.6.2 Sleutelmateriaal & PKI

Deze sectie beschrijft de eisen aan digitale handtekeningen, sleutelbeheer en de publieke sleutelinfrastructuur. Het betreft de fundamenten waarop het authenticatieproces is gebouwd: hoe partijen cryptografisch bewijzen wie ze zijn en hoe sleutelmateriaal wordt beheerd.

ID	Requirement	Rationale
AUTH-009	Deelnemers aan het netwerk (issuers, verifiers, dienstverleners, zorginstellingen) MOETEN claims kunnen ondertekenen met digitale handtekeningen **met gebruik van erkende cryptografische algoritmen**	Vertrouwen tussen partijen wordt gevestigd via cryptografisch bewijs. Digitale handtekeningen stellen partijen in staat verifieerbare uitspraken te doen
AUTH-010	Er MOET een publieke sleutelinfrastructuur bestaan waarmee elke partij het sleutelmateriaal van een andere partij kan achterhalen	Verifiers moeten publieke sleutels kunnen verkrijgen om handtekeningen op claims en assertions te valideren. Dit mag niet afhankelijk zijn van de beschikbaarheid van de ondertekende partij op het moment van verificatie
AUTH-011	Elke deelnemer aan het netwerk MOET een unieke technische identifier hebben die herleidbaar is naar het bijbehorende sleutelmateriaal	Om een handtekening te verifiëren moet de verifier de publieke sleutel van de ondertekenaar kunnen opzoeken via een stabiele technische identifier
AUTH-012	Technische identifiers MOETEN gescheiden zijn van business identifiers (zoals URA, KVK, UZI)	Business identifiers dienen andere doeleinden (wettelijke registratie, professionele kwalificatie) en hebben een andere levenscyclus en governance. Koppeling creëert afhankelijkheden en beperkingen
AUTH-013	De resolutie van identifiers naar sleutelmateriaal MOET beveiligd zijn tegen manipulatie en impersonatie, en de binding tussen een technische identifier en het bijbehorende sleutelmateriaal MOET cryptografisch verifieerbaar zijn	Deze resolutie staat aan de basis van het vertrouwen in het stelsel. De beveiliging moet proportioneel zijn aan de rol van de partij in het stelsel
AUTH-014	Elke partij is juridisch eigenaar van het eigen sleutelmateriaal; sleutels en certificaten MOGEN NIET gedeeld worden tussen organisaties. Het operationele beheer van sleutelmateriaal MAG worden uitbesteed, mits dit expliciet is geautoriseerd	Juridisch eigenaarschap waarborgt verantwoordelijkheid en aansprakelijkheid. Dit is fundamenteel anders dan de huidige situatie waarin private keys van certificaten vaak verspreid zijn over partijen die het certificaat technisch nodig hebben. Uitbesteding van operationeel beheer is toegestaan, maar het eigenaarschap en de verantwoordelijkheid blijven bij de organisatie
AUTH-015	Organisaties MOETEN meerdere sleutels kunnen beheren voor verschillende doeleinden (bv. ondertekenen van credentials vs. ondertekenen van presentaties). Het beoogde gebruik van elke sleutel MOET vastgelegd zijn in metadata. Hergebruik van één sleutel voor meerdere doeleinden	Scheiding van sleutels beperkt de impact van compromittering en maakt fijnmazige delegatie mogelijk. Een partij die geautoriseerd is om presentaties te ondertekenen mag niet automatisch credentials kunnen uitgeven

	of vertrouwensdomeinen is NIET TOEGESTAAN	
AUTH-016	Elke cryptografische sleutel MOET één expliciete juridische eigenaar hebben; delegatie van gebruik is niet gelijk aan delegatie van eigenaarschap	Nodig voor aansprakelijkheid, incidentafhandeling en intrekking
AUTH-017	Sleutelmateriaal MOET vervangbaar zijn zonder wijziging van de bijbehorende technische identifier, waar de situatie dit vereist	Voor sommige rollen in het stelsel (bv. issuers) is sleutelrotatie essentieel vanwege de langdurige geldigheid van uitgegeven claims. Voor andere rollen (bv. holders met kortlopende presentaties) is de noodzaak minder groot. De identifier moet stabiel kunnen blijven om referenties en audithistorie te behouden, maar niet elke technische identifier-methode ondersteunt dit (bv. did:key)
AUTH-018	Intrekking van sleutels die bedoeld zijn voor het ondertekenen van claims MOET mogelijk zijn per individuele sleutel en MOET direct detecteerbaar zijn door verifiërende partijen	Gecompromitteerde signing-sleutels hebben de grootste impact omdat de claims die ermee ondertekend zijn langdurig geldig kunnen zijn. De eisen aan intrekking van sleutels voor andere doeleinden (bv. presentaties) vereisen nader onderzoek (zie OV-013)
AUTH-0181	Sleutelmateriaal (met name private keys) MOET beschermd worden tegen ongeautoriseerde toegang en gebruik, conform actuele beveiligingsstandaarden (bijv. gebruik van HSM of secure enclave waar passend)	Private keys vormen de kern van het vertrouwen in het stelsel: wie de sleutel bezit, kan zich voordoen als de rechtmatige eigenaar en geldige handtekeningen produceren. Adequate bescherming van sleutelmateriaal zoals HSM's of secure enclaves is essentieel om ongeautoriseerd gebruik te voorkomen en het vertrouwen in het gehele netwerk te waarborgen.

7.6.3 Verificatie & presentatie van delegatie

Sectie 5.3 beschrijft de inhoudelijke eisen aan het delegatiemodel. Deze sectie beschrijft hoe delegaties en claims worden gepresenteerd en geverifieerd als onderdeel van het authenticatieproces.

ID	Requirement	Rationale
AUTH-019	De rollen zorgaanbieder en dienstverlener MOETEN altijd als apart identificeerbare entiteiten zichtbaar zijn in het authenticatieproces en in de gepresenteerde authenticatiebewijzen, en er MOET altijd een expliciete delegatie tussen hen bestaan	Ongeacht wie technisch welke sleutels beheert of hoe de operationele inrichting eruitziet, moeten beide rollen en hun relatie expliciet zijn. Dit geldt ook wanneer een zorginstelling haar eigen dienstverlener is
AUTH-020	Claims die in een enkele presentatie worden gecombineerd MOETEN altijd betrekking hebben op hetzelfde subject (dezelfde geïdentificeerde organisatie)	Het combineren van claims over verschillende subjecten in één presentatie leidt tot complexe validatieregels en vergroot het risico op fouten bij verificatie
AUTH-021	Een verifiërende partij MOET het delegatiebewijs valideren als onderdeel van het authenticatie proces voordat zij	Gevoelige informatie mag niet gelekt worden aan ongeautoriseerde partijen. Verificatie moet plaatsvinden vóór de inhoudelijke uitwisseling

	claims of beschermde gegevens accepteert	
AUTH-022	Verifiërende partijen MOETEN de intrekkingsstatus van delegatiebewijzen kunnen vaststellen zonder synchrone calls naar de uitgever	Intrekking van een delegatie heeft een cascade-effect op alle claims die eronder vallen, wat het anders maakt dan intrekking van een individuele claim. Statusinformatie moet asynchroon opvraagbaar en cacheable zijn
AUTH-023	Dienstverleners die namens zorginstellingen opereren MOETEN verifieerbare delegatiebewijzen publiceren op een vindbare locatie	Verifiërende partijen moeten delegatiebewijzen kunnen verkrijgen en controleren vóór het initiëren van een authenticatieverzoek
AUTH-024	Authentiserende partijen MOETEN de delegatie van een zorginstelling aan een dienstverlener kunnen verifiëren voordat zij identiteitsclaims of beschermde gegevens versturen	Partijen mogen geen gevoelige data lekken aan ongeautoriseerde partijen. Delegatieverificatie moet plaatsvinden voordat de raadplegende partij claims of patiëntdata verstuurt aan de bronhouder

7.6.4 Wallet-beheer

In de context van dit document is een wallet de plek waar een partij sleutels, claims en delegaties beheert. Deze sectie beschrijft de eisen aan het beheer van wallets. De vraag wie welke wallet beheert heeft directe gevolgen voor de operationele last, beveiliging en autonomie van de betrokken partijen.

ID	Requirement	Rationale
AUTH-025	Elke partij (zorginstelling, dienstverlener) MOET in staat zijn een eigen wallet te beheren, inclusief het beheer van sleutelmateriaal, claims en delegatiebewijzen	Autonomie en onafhankelijkheid zijn essentieel; partijen mogen niet gedwongen worden hun claims en sleutels door een andere partij te laten beheren
AUTH-026	Het MOET voor een verifiërende partij niet uitmaken wie het operationele beheer van een wallet voert, mits de presentatie cryptografisch geldig is en de delegatiebewijzen correct zijn	De verificatielogica moet gebaseerd zijn op cryptografische validiteit, niet op kennis van de interne organisatie van de presenterende partij

7.6.5 Presentatie-model

Deze sectie beschrijft de eisen aan hoe claims worden aangeboden aan een verifiërende partij. In dit hoofdstuk gebruiken we de term "claim" voor een verifieerbare uitspraak over een subject, en "presentatie" voor het geheel aan claims dat in een transactie wordt aangeboden. Hiermee wordt geen specifieke technologie (zoals W3C Verifiable Credentials) voorgeschreven.

ID	Requirement	Rationale
AUTH-027	Het presentatie-model MOET een duidelijke scheiding aanbrengen tussen de identiteit van de dienstverlener en de identiteit van de zorginstelling namens wie gehandeld wordt	Voor audit en compliance moet ondubbelzinnig zijn wie de handeling uitvoert en namens wie (zie IDENT-018)
AUTH-028	Het presentatie-model MOET ondersteunen dat claims over zowel de dienstverlener als de zorginstelling in dezelfde transactie worden overgedragen	Een verifiërende partij heeft in één transactie informatie nodig over zowel de handelende partij als de verantwoordelijke organisatie
AUTH-029	Claims die in een presentatie zijn opgenomen MOETEN cryptografisch gebonden zijn aan de	Losse claims die buiten een presentatie hergebruikt kunnen worden, creëren

	presentatie, zodat ze niet herbruikbaar zijn buiten de context van die presentatie	risico's op replay-aanvallen en ongeautoriseerd gebruik
AUTH-030	Authenticiteit van de presentatie Een verifiërende partij MOET kunnen aantonen dat de presentatie daadwerkelijk afkomstig is van de geclaimde dienstverlener en zorginstelling	De eis waarborgt dat een verifiërende partij kan vertrouwen op de oorsprong van de gepresenteerde claims.

7.6.6 OAuth-profiel

Het OAuth 2.0-framework wordt gebruikt als basis voor het authenticatieprotocol. In OAuth zijn de volgende rollen relevant:

- **Client**: het systeem dat namens een gebruiker of organisatie toegang vraagt tot beschermde gegevens. In de context van dit stelsel is de client doorgaans het systeem van de dienstverlener.
- **Authorization Server (AS)**: het systeem dat de identiteit en bevoegdheden van de client vaststelt en een access token uitgeeft. De AS opereert namens de bronhouder (de zorginstelling die de gegevens beheert).
- **Resource Server (RS)**: het systeem dat de beschermde gegevens beheert en toegang verleent op basis van een geldig access token. De RS opereert eveneens namens de bronhouder.
- **Relying Party**: de partij die vertrouwt op de informatie in het access token om autorisatiebeslissingen te nemen. In de praktijk is dit doorgaans de resource server.

De belangrijkste interactie is het token request: de client stuurt claims over zichzelf en de partijen namens wie het handelt naar de authorization server, die na verificatie een access token uitgeeft. Dit access token wordt vervolgens gebruikt bij de resource server om toegang te krijgen tot gegevens.

Belangrijk: OAuth authentiseert niet alleen de eindgebruiker maar ook de client zelf. In dit stelsel betekent dat dat de dienstverlener zich als client identificeert en authenticeert bij de authorization server, op dezelfde wijze als andere deelnemers in het stelsel: via verifieerbare claims uitgegeven door autoritatieve bronnen.

ID	Requirement	Rationale
OAUTH-001	Het OAuth-profiel MAG NIET vereisen dat clients vooraf geregistreerd of geconfigureerd worden bij elke authorization server, noch dat authorization servers lijsten van goedgekeurde partijen bijhouden	Traditionele OAuth-clientregistratie en onderhouden lijsten schalen niet wanneer veel clients met veel authorization servers moeten communiceren. Clienttoelating moet worden bepaald op basis van verifieerbare claims die at runtime worden gepresenteerd
OAUTH-002	Clients MOETEN verifieerbare claims over hun identiteit en kwalificaties kunnen meesturen als onderdeel van het token request. Hierbij MOET onderscheid gemaakt worden tussen de technische identifier van de client en de business identifiers van de partijen namens wie het handelt	Autorisatiebeslissingen kunnen afhangen van clienteigenschappen (bv. NEN 7510-certificering). De scheiding tussen technische en business identifiers voorkomt ongewenste koppeling en waarborgt flexibiliteit
OAUTH-003	Een vertrouwde autoriteit MOET verifieerbare claims kunnen uitgeven over de identiteit en capaciteiten van een client (bv. softwarecertificering, netwerklidmaatschap)	Authorization servers hebben zekerheid nodig dat clients aan bepaalde standaarden voldoen. Een netwerkautoriteit of certificeringsinstantie kan verifieerbare

		claims leveren zonder bilaterale registratie
OAUTH-004	Het OAuth-profiel MOET een back-channel token request flow ondersteunen (zonder user-agent redirect)	Veel zorginteracties zijn systeem-naar-systeem zonder gebruikersbetrokkenheid (AUTH-004). Back-channel flows verbeteren ook de gebruikerservaring door herhaalde browser-redirects te vermijden (AUTH-005)
OAUTH-005	Het token request MOET ondersteunen dat de client claims presenteert over twee subjecten: de zorginstelling namens wie gehandeld wordt en de dienstverlener die de handeling uitvoert. Claims over een medewerker van de zorginstelling vallen onder het subject van de zorginstelling	Een verifiërende partij moet in één transactie kunnen vaststellen wie de verantwoordelijke organisatie is en wie de handeling uitvoert. De medewerker ondertekent niet zelf (zie AUTH-005), maar wordt vertegenwoordigd via een delegatie aan de zorginstelling
OAUTH-006	Het token request MOET een duidelijk onderscheid maken tussen de partij die het token aanvraagt (client) en de partijen namens wie toegang wordt gevraagd (subjecten)	Delegatiescenario's vereisen expliciete identificatie van alle betrokken partijen (IDENT-018). Clientauthenticatie en de autorisatie-grant dienen verschillende doelen
OAUTH-007	Claims die in het token request worden gepresenteerd MOETEN cryptografisch ondertekend zijn door de juiste partij	De verifier moet kunnen valideren dat claims afkomstig zijn van de geclaimde uitgever en gepresenteerd worden door de legitieme houder
OAUTH-008	Access tokens MOETEN gebonden zijn aan de business identifier (URA) van de zorginstelling waarvoor het token is uitgegeven. De AS is per URA adresseerbaar via een identifier in het token endpoint path	Een authorization server kan namens meerdere zorginstellingen opereren. Het token moet ondubbelzinnig de verantwoordelijke zorginstelling identificeren. De URA als audience voorkomt dat tokens bruikbaar zijn buiten de beoogde context
OAUTH-009	Het OAuth-profiel MOET scope-gebaseerde toegangscontrole ondersteunen, afgestemd op use-case-specifieke eisen	Verschillende toepassingen vereisen verschillende toegangsniveaus. Scope-gebaseerde toegangscontrole is vereist voor compatibiliteit met SMART-on-FHIR en andere zorg-OAuth-profielen
OAUTH-010	Access tokens MOETEN cryptografisch gebonden zijn aan de client, en de client MOET deze binding aantoonbaar maken bij elk gebruik van het token. Dit mechanisme MOET replay-bescherming bevatten	Bearer tokens kunnen gestolen en hergebruikt worden. Cryptografische token binding waarborgt dat alleen de legitieme client het token kan gebruiken. Replay-bescherming voorkomt dat onderschepte bewijzen hergebruikt worden
OAUTH-011	Het OAuth-profiel MOET ondersteunen dat eindgebruiker-authenticatie losgekoppeld is van de token request flow, zodat een gebruiker eenmaal per sessie authenticeert en het resultaat herbruikbaar is in daaropvolgende back-channel verzoeken. Wanneer interactieve authenticatie vereist is (bv. initiële login, step-up) MOET een front-channel flow beschikbaar zijn	Zorgverleners moeten eenmaal per sessie authenticeren (AUTH-005). Een front-channel flow is nodig voor scenario's waar interactie met de gebruiker vereist is, bv. via een Identity Provider

OAUTH-012	Het OAuth-profiel MOET authorization servers ondersteunen die namens meerdere zorginstellingen opereren (multi-tenant)	Veel zorginstellingen maken gebruik van gedeelde infrastructuur of managed services. Het token request moet de specifieke organisatiecontext identificeren
OAUTH-013	Authorization servers MOETEN de delegatierelaties met de zorginstellingen waarvoor zij opereren publiceren op een vindbare locatie, en deze MOETEN cryptografisch verifieerbaar zijn met het sleutelmateriaal van de zorginstelling zonder runtime-contact met de zorginstelling	Clients moeten delegatie-informatie kunnen verkrijgen en verifiëren voordat zij identiteitsclaims versturen (AUTH-024). Ondertekende of zelfverklaarde delegatieclaims kunnen niet vertrouwd worden
OAUTH-014	Access tokens MOETEN opaque zijn voor clients	Clients mogen tokeninhoud niet parsen of ervan afhankelijk zijn. Dit ontkoppelt de clientimplementatie van het interne tokenformaat van de authorization server
OAUTH-015	Resource servers MOETEN access tokens kunnen valideren en identiteitsclaims kunnen extraheren	Resource servers hebben identiteitsinformatie nodig voor autorisatiebeslissingen en auditlogging
OAUTH-016	Het OAuth-profiel MOET intrekking van claims die in token requests worden gebruikt ondersteunen. Intrekkingsstatus MOET controleerbaar zijn zonder synchrone calls naar de uitgever	Gecompromitteerde of ingetrokken claims moeten detecteerbaar zijn. Intrekkingscontroles mogen geen runtime-afhankelijkheden creëren
OAUTH-017	Token requests MOETEN minimale disclosure ondersteunen -- alleen de claims die noodzakelijk zijn voor de specifieke transactie MOGEN worden opgenomen	Privacy-by-design vereist dat verifiers alleen de informatie ontvangen die nodig is voor hun autorisatiebeslissing (AUTH-003)
OAUTH-018	Het OAuth-profiel MOET sleutelrotatie ondersteunen zonder wijzigingen aan identifiers of configuratie bij andere partijen	Operationele beveiliging vereist periodieke sleutelvervanging. De token request flow moet bijgewerkt sleutelmateriaal accommoderen zonder bestaande relaties te verstoren (AUTH-017)

7.7 Eisen aan Autorisatie

<< referentie naar autorisaties in AORTA >>

7.8 Eisen aan Adressering

[Dit onderwerp is nog ter discussie voor de Nuts x AORTA/LSP]

De adresseringsfunctie is gebaseerd op het IHE mCSD-profiel en uitgewerkt in de Care Services Directory IG. Onderstaande requirements beschrijven de eisen die de harmonisatie stelt aan (de inrichting van) deze adresseringsfunctie.

ID	Requirement	Rationale
1	Technische endpoints moeten op basis van een URA vindbaar zijn	Partijen uit beide netwerken moeten elkaars systemen kunnen vinden zonder voorkennis van de technische infrastructuur
2	Het LSP MOET de endpoints van haar achterliggende systemen kunnen publiceren in de Care Services Directory, zonder dat die	Het LSP fungeert als knooppunt; achterliggende partijen mogen niet belast worden met de harmonisatie.

	achterliggende systemen hier zelf actie voor hoeven te ondernemen	
3	Nuts-nodes MOETEN hun eigen endpoints publiceren in de Care Services Directory	Elke Nuts-node functioneert als zelfstandig knooppunt en is verantwoordelijk voor de eigen registratie
4	Een zoekend systeem MOET op basis van een URA-nummer en een toepassing of data-type het juiste endpoint kunnen vinden, ongeacht achter welk knooppunt dit endpoint zich bevindt	Het maakt voor de zoekende partij niet uit via welk knooppunt een zorginstelling bereikbaar is
5	De relatie tussen een knooppunt en de zorginstellingen waarvoor het endpoints publiceert MOET verifieerbaar zijn	Voorkomen dat ongeautoriseerde partijen endpoints registreren namens een zorginstelling
6	De adresseringsfunctie MOET nieuwe knooppunten en netwerken kunnen accommoderen zonder wijzigingen aan de bestaande registraties	Schaalbaarheid en toekomstbestendigheid
7	Endpoints MOETEN vindbaar zijn op basis van het type dienst (of data type) dat zij ondersteunen	Een zoekend systeem moet kunnen filteren op het type gegevensuitwisseling dat het wil doen, ongeacht via welk knooppunt
8	Voor elke combinatie van **zorgaanbieder (URA-nummer)** en **diensttype (service type of data type)** MOET ten minste één geldig technisch endpoint in de Care Services Directory geregistreerd en vindbaar zijn.	Een zoekend systeem moet op basis van de identificatie van een zorgaanbieder en het type gegevensuitwisseling ondubbelzinnig kunnen bepalen via welk technisch endpoint communicatie moet plaatsvinden. Dit voorkomt ambiguïteit en ondersteunt interoperabele en geautomatiseerde routering van berichten tussen netwerken.

7.9 Eisen aan Logging & Transparantie

<<Uitwerking Wulf: o.b.v. NEN 7513>>

7.10 Open onderzoeksvragen & impactanalyse

- Deze sectie bevat een overzicht van de openstaande designkeuzes en onderzoeksvragen die voortkomen uit de requirements in de voorgaande secties. Bij elke vraag wordt beschreven welke impact de mogelijke keuzes hebben op de oplossing als geheel.

7.10.1 Credential-model

ID	Vraag	Referenties	Impact
OV-001	Moet een Verifiable Credential over een zorginstelling los staan van de dienstverlener die het gebruikt, of wordt de holder opgenomen in het VC?	AUTH-004, AUTH-006	Bij een los VC hoeft een zorginstelling per issuer maar één VC te ontvangen, ongeacht het aantal dienstverleners. Bij opname van de holder in het VC ontstaan er meerdere variaties van hetzelfde VC bij meerdere dienstverleners. Dit raakt schaalbaarheid en beheerslast
OV-002	Wie initieert het ophalen van VCs bij issuers: de dienstverlener (GTK) via een delegation, of een tekenbevoegd persoon van de zorginstelling zelf?	AUTH-005, ID-001	Dit bepaalt of een dienstverlener zelfstandig credentials kan verwerven of dat de zorginstelling hier altijd bij betrokken moet zijn. Raakt de operationele last voor zorginstellingen en de autonomie van dienstverleners
OV-003	Moet het subject.id in een VC altijd verwijzen naar de partij waar het VC over gaat?	AUTH-001	Dit is een semantische eis die bepaalt hoe VCs gestructureerd worden. Afwijking hiervan kan leiden tot interpretatieverschillen bij verifiers

7.10.2 Presentatie-model

ID	Vraag	Referenties	Impact
OV-004	Levert een initiërende holder (GTK) één VP op (met daarin alle benodigde VCs), of twee aparte VPs (één van zichzelf en één namens de zorginstelling)?	AUTH-001, AUTH-008	Bij één VP moeten er niet-standaard business rules worden geïntroduceerd omdat niet alle VCs als subject de issuer van de VP hebben. Twee VPs maken de scheiding tussen partijen expliciet en volgen het standaardmodel, maar verhogen de complexiteit van de transactie. Dit raakt het OAuth-profiel en de token request flow

7.10.3 Wallet-beheer

ID	Vraag	Referenties	Impact
OV-005	Beheert de dienstverlener zowel de wallet van de zorginstelling als van zichzelf, of beheren zij elk hun eigen wallet?	AUTH-006, AUTH-012	Gedeeld beheer is operationeel eenvoudiger maar creëert afhankelijkheid en risico bij de dienstverlener. Gescheiden beheer is veiliger maar vereist meer technische volwassenheid bij zorginstellingen, met name in de VVT-sector
OV-006	Moet het voor de verifier uitmaken wie het beheer over een wallet heeft?	AUTH-003, AUTH-005	Als de verifier dit onderscheid niet hoeft te maken, vereenvoudigt dit de verificatielogica. Maar het kan gevolgen hebben voor de audittrail en verantwoording

7.10.4 Adressering

ID	Vraag	Referenties	Impact
OV-007	Hoe wordt de routering ingericht wanneer een zorginstelling via meerdere knooppunten bereikbaar is en een zoekend systeem op basis van URA en toepassing het juiste endpoint moet vinden?	ADR-004, ADR-005	Dit bepaalt de complexiteit van de Care Services Directory en heeft gevolgen voor de lookup-logica bij zoekende systemen

7.10.5 Lokalisatie

ID	Vraag	Referenties	Impact
OV-008	Hoe worden de authenticatie-attributen die de NVI vereist (URA, organisatietype, UZI/DEZI, rolcode) afgeleid uit het geharmoniseerde authenticatiemodel voor partijen die geen UZI-pas hebben?	LOK-004, HAR-005	Zonder oplossing hiervoor kunnen VVT-partijen de NVI niet bevragen. Dit is een directe blokkade voor gelijkwaardige deelname

7.10.6 Sleutelmateriaal & beveiliging

ID	Vraag	Referenties	Impact
OV-009	In hoeverre is hardware-gebaseerde sleutelgeneratie en -opslag (HSM, smartcard, secure enclave) vereist, gegeven dat dit de toetredingsdrempel verhoogt voor met name de VVT-sector?	NFR 2, NFR 3, HAR-005, HAR-007	Een harde hardware-eis blokkeert mogelijk partijen die nu geen toegang hebben tot dergelijke middelen. Zonder hardware-eis ontstaan risico's rondom sleutelcompromittering

OV-010	Is sterke gebruikersauthenticatie (2FA) vóór sleutelgebruik vereist, en hoe verhoudt dit zich tot geautomatiseerde systemen zonder eindgebruiker?	NFR 5, AUTH-004	Een 2FA-eis voorkomt ongeautoriseerd signing maar maakt machine-to-machine communicatie complexer of onmogelijk
OV-011	Moeten er vertrouwensniveaus worden gedefinieerd waarbinnen verschillende eisen gelden voor sleutelbeheer, intrekking en beveiliging, afhankelijk van de rol van de sleutel in het stelsel?	AUTH-013, AUTH-015, AUTH-017, AUTH-018	Signing-sleutels voor langlopende credentials hebben een ander risicoprofiel dan sleutels voor kortdurende presentaties. Uniforme eisen kunnen ofwel te streng zijn voor lichtgewicht rollen, ofwel te soepel voor kritieke rollen

7.10.7 Dienstverlener delegatie

ID	Vraag	Referenties	Impact
OV-012	Moet er een centraal register van toepassingen/diensten komen, en wie beheert dit?	OAUTH-009, IDENT-015	Bepaalt hoe de dienstenlijst in het ServiceProviderCredential wordt samengesteld en bijgehouden. Raakt de rol van de stelselhouder
OV-13	Hoe verhouden de scope-identifiers in credentials zich tot SMART-on-FHIR scopes en NVI data types? Is een uniforme taxonomie haalbaar, of is een mapping tussen bestaande concepten realistischer?	OAUTH-009, LOK-004	Bepaalt de complexiteit van scope-validatie bij de authorization server en de inspanning die nodig is om bestaande systemen aan te sluiten
OV-14	Kunnen deelnemers onderling toepassingen afspreken buiten de stelselhouder om, en hoe wordt dit in de credentials uitgedrukt?	IDENT-015, HAR-011	Raakt de balans tussen centrale governance en decentrale autonomie. Bij een strikt centraal model moet elke nieuwe toepassing langs de stelselhouder; bij een decentraal model ontstaat het risico op fragmentatie

8 Oplossingsrichtingen

8.1 Inleiding

Dit hoofdstuk beschrijft de oplossingsrichting voor de harmonisatie van de vertrouwensmodellen van Nuts en AORTA. Het bouwt voort op de requirements uit de voorgaande hoofdstukken en beschrijft per onderwerp de gekozen richting. Waar de requirements beschrijven *wat* de oplossing moet kunnen, beschrijft dit hoofdstuk *hoe* dat wordt ingevuld.

De oplossing is gebaseerd op W3C Verifiable Credentials en Decentralized Identifiers als fundament voor het identiteits- en authenticatiemodel, gecombineerd met een OAuth 2.0-profiel voor de technische authenticatiestroom. Deze keuze maakt het mogelijk om de bestaande certificaatinfrastructuur te hergebruiken en tegelijkertijd een flexibel en toekomstbestendig model neer te zetten.

Dit hoofdstuk begint met een ontologie die de partijen, rollen en relaties in het model visueel en tekstueel beschrijft (8.2). Vervolgens wordt het identiteitsmodel uitgewerkt: welke DID-methoden worden gebruikt en welke credentials er bestaan (8.3). Daarna wordt beschreven hoe credentials worden gepresenteerd en geverifieerd (8.4), hoe het OAuth-profiel is ingericht (8.5) en hoe het sleutelmateriaal wordt beheerd (8.6). Het hoofdstuk sluit af met de oplossingsrichting voor adressering (8.7) en lokalisatie (8.8).

Waar nog geen consensus is of waar designkeuzes nog open staan, wordt verwezen naar de onderzoeksvragen in sectie 7. Bij een aantal van deze vragen wordt in dit hoofdstuk wel een voorkeursrichting beschreven.

8.2 Was 6.4 en 6.5

Was 6.3.3

8.2.1 Trust Framework and Governance

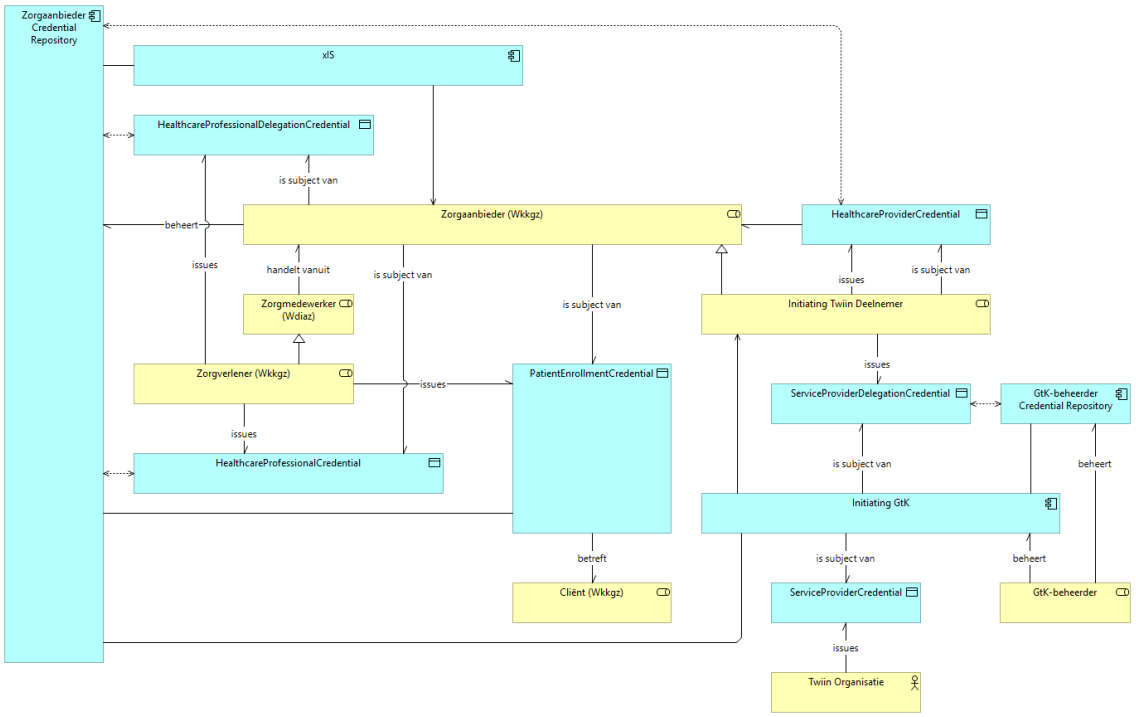
Authoritative Issuers and Lifecycle Management

- Verifiable Credentials containing business identifiers MUST be issued by ***authoritative issuers***.
- The authoritative issuer MUST:
    - Register DID bindings,
    - Manage lifecycle (issuance, update, revocation, expiry),
    - Expose revocation/status information.

This role is functionally equivalent to the UZI-register, certificate management, and CRL/OCSP mechanisms in AORTA.

8.3 Gewenste procesinrichting (was 6.4)

In de tekening hieronder worden de Verifiable Credentials weergegeven die nodig zijn voor een Initiërende Twiin Deelnemer (inclusief de Initiërende GtK en de GtK-beheerder).



Met betrekking tot verifiable credentials, gelden de volgende definities (zie ook W3C).

1. Entiteit: alles waarnaar in uitspraken kan worden verwezen als een abstract of concreet zelfstandig naamwoord. Entiteiten omvatten, maar zijn niet beperkt tot, personen, organisaties en fysieke objecten. Elke entiteit kan rollen vervullen binnen het ecosysteem.
2. Uitgever: een rol die een entiteit kan vervullen door beweringen te doen over een of meer onderwerpen, een verifieerbare referentie te creëren op basis van deze beweringen en de verifieerbare referentie door te geven aan een houder.
3. Onderwerp: een ding waarover beweringen worden gedaan.
4. Houder: een rol die een entiteit kan vervullen door in het bezit te zijn van een of meer verifiable credentials en daaruit verifieerbare presentaties te genereren. Een houder is vaak, maar niet altijd, een subject van de verifieerbare referenties die hij in bezit heeft. Houders slaan hun referenties op in referentieopslagplaatsen.
5. Referentieopslagplaats: software, zoals een bestandssysteem, opslagkluis of persoonlijke portemonnee voor verifieerbare referenties, die de verifieerbare referenties van houders opslaat en de toegang daartoe beveiligt.
6. Verifieerbare referentie: een referentie die niet kan worden gemanipuleerd en waarvan het auteurschap cryptografisch kan worden geverifieerd. Verifieerbare referenties kunnen worden gebruikt om verifieerbare presentaties te maken, die ook cryptografisch verifieerbaar kunnen zijn.
7. Verifieerbare weergave: een fraudebestendige weergave van informatie die zodanig is gecodeerd dat de herkomst van de gegevens na een cryptografisch verificatieproces als betrouwbaar kan worden beschouwd. Bepaalde soorten verifieerbare weergaven kunnen gegevens bevatten die zijn samengesteld op basis van, maar niet bestaan uit, de oorspronkelijke verifieerbare referenties (bijvoorbeeld zero-knowledge-bewijzen).

HealthcareProfessionalDelegationCredentials en PatientEnrollmentCredentials worden uitgegeven door een zorgverlener en worden opgeslagen in een Zorgaanbieder Credential Repository.

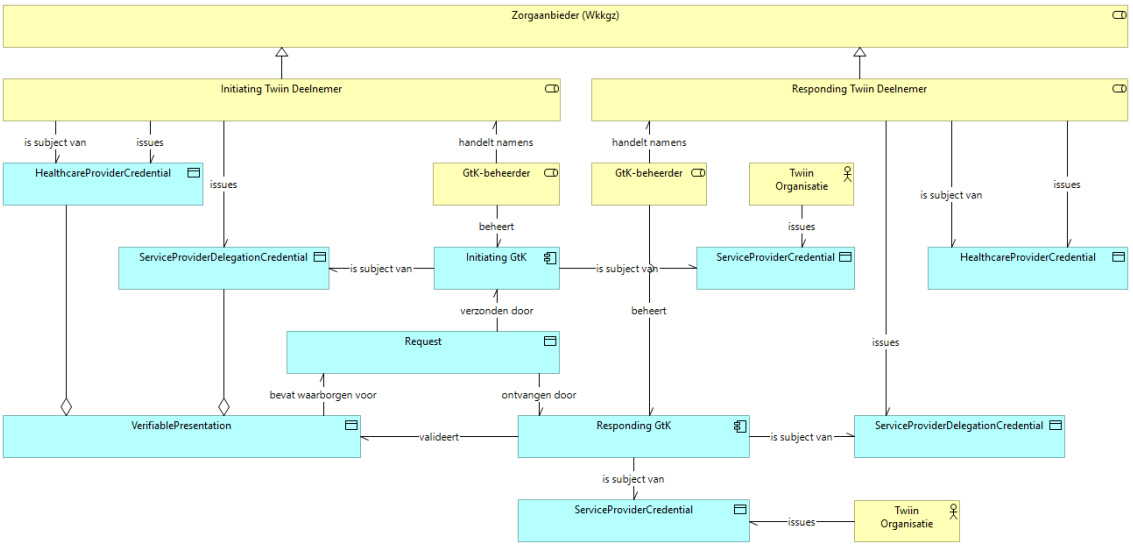
Een HealthcareProfessionalDelegationCredential bevat gegevens over een delegatie die door een zorgverlener is uitgevoerd. Een PatientEnrollmentCredential bewijst dat een bepaalde patiënt bij een bepaalde zorgverlener is geregistreerd.

HealthcareProviderCredentials en ServiceProviderDelegationCredentials worden uitgegeven door een zorgorganisatie. De ServiceProviderDelegationCredential wordt opgeslagen in een GtK-beheerder Credential Repository. De HealthcareProviderCredential wordt opgeslagen in een Zorgaanbieder Credential Repository.

Een HealthcareProviderCredential bewijst dat een bepaalde zorgorganisatie bestaat en dat er een bepaalde URA aan is toegewezen als identificatiecode. Een ServiceProviderDelegationCredential bewijst dat de zorgorganisatie de verantwoordelijkheid voor bepaalde handelingen heeft gedelegeerd aan een GtK, geïdentificeerd door een ServiceProviderCredential. Een ServiceProviderCredential wordt uitgegeven door een vertrouwde organisatie (bijv. de Twiin-organisatie).

Een Initiating GtK kan Verifiable Credentials ophalen uit beide Credential Repositories en door zijn ServiceProviderDelegationCredential toe te voegen, mag hij deze credentials presenteren aan een Responding GtK.

In de onderstaande afbeelding staan de verifiable credentials vermeld die vereist zijn voor GtK-beheerders. **Let op**: de weergegeven referenties overlappen gedeeltelijk met de volledige set referenties die vereist is voor een initiërende Twiin-deelnemer.



Zoals eerder vermeld, moet de initiërende GtK aantonen dat hij bevoegd is om namens de initiërende Twiin Deelnemer op te treden door een aantal Verifiable Credentials aan een reagerende GtK te tonen.

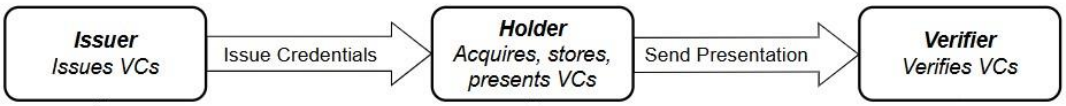
Omgekeerd moet een Responding GtK aan een Initiating GtK bewijzen dat hij bevoegd is om namens de Responding Twiin Deelnemer te handelen. Hiervoor gebruikt de Responding GtK ook een HealthcareProviderCredential, een ServiceProviderCredential en een ServiceProviderDelegationCredential.

8.3.1 Actoren

Issuers: één of meer vertrouwde partijen die Verifiable Credentials (VC's) uitgeven, waarbij elke referentie specifieke feiten of machtigingen bevestigt (bijv. identiteit van de organisatie, rol, delegatie).

Holder: Een enkele entiteit die referenties ontvangt, opslaat, beheert en presenteert die zijn uitgegeven door meerdere issuers. De holder handelt namens zichzelf of namens een andere partij op basis van de referenties die hij bezit.

Verifier: Een vertrouwende partij die een verifieerbare presentatie (VP) ontvangt en de gepresenteerde referenties evalueert om een autorisatie- of toegangsbeslissing te nemen.



8.3.2 Proces overzicht

8.3.2.1 Credential uitgifte

Elke Issuer geeft onafhankelijk één of meer Verifiable Credentials uit aan de Holder.

- Credentials worden cryptographisch ondertekend door de Issuer.
- Elke credential heeft een eigen:
  - issuer
  - subject
  - validity period
  - scope en constraints.
- Credentials zijn ***context onafhankelijk*** en **herbruikbaar voor verschillende op zichzelf staande use cases**.

Voorbeelden:

- Een Organization VC uitgegeven door een zorgaanbieder.
- Een Delegation VC uitgegeven door een zorgaanbieder waarmee de Holder namens de zorgaanbieder mag handelen.
- Een Role of Attribute VC uitgegeven door een vertrouwde autoriteit.

8.3.2.2 Credential opslag en management

De Holder:

- Verzameld credentials van meerdere issuers.
- Bewaard credentials in een beveiligde wallet of beveiligde opslag.
- Beheert de levenscyclusaspecten zoals:
  - geldigheid;
  - intrekkingsstatus;
  - vernieuwing.

De Holder is verantwoordelijk voor het selecteren van de relevante inloggegevens voor een bepaalde interactie.

8.3.2.3 Voorbereiding van de Presentatie

Bij een interactie met een Verifier, de Holder:

- Selecteert de houder de vereiste referenties op basis van:
  - de gevraagde dienst;

- de beoogde actie;
- de vereisten en het beleid van de verifier.

- Valideert de geselecteerde referenties vóór gebruik
- Stelt een verifieerbare presentatie (VP) samen die:
  - één of meer referenties bevat;
  - context toevoegt tijdens de uitvoering (doelgroep, doel, reikwijdte, transactie);
  - de intentie en actie van de houder weergeeft.

De VP vertegenwoordigt een **moment specifieke assertion**, afgeleid van langdurige referenties.

8.3.2.4 Presentatie en Bewijs

De Holder presenteert de Verifiable Presentation (VP) aan de Verifier en:

- ondertekent cryptografisch de VP;
- bewijst de controle over de Holder-identificatie en sleutels;
- past optioneel selectieve openbaarmaking of minimalisering toe.

De handtekening van de VP bevestigt:

- de verantwoordelijkheid van de Holder;
- de non-repudiation van de gepresenteerde assertion.

8.3.2.5 Verificatie en handhaving

De Verifier:

- Verifieert de VP-ondertekening
- Valideert elke ingesloten credential:
  - issuer trust;
  - ondertekening validatie;
  - validatie periode;
  - intrekkingsstatus.
- Evalueert delegatie chains en autorisatie scope
- Past lokaal beleid toe om te bepalen of de gevraagde actie is toegestaan.

Autorisatiebeslissingen zijn gebaseerd op verifieerbaar bewijs, niet op impliciet vertrouwen in de Holder.

8.3.3 Belangrijkste architectuurprincipes

- Referenties worden eenmalig uitgegeven en vele malen gebruikt

- Asserties worden per interactie aangemaakt

- Uitgevers nemen niet deel aan transacties tijdens de uitvoering

- De Holder is de actieve partij en verantwoordelijk voor de acties

- De Verifier neemt een onafhankelijke vertrouwensbeslissing.

8.3.4 Geconsolideerd identiteits- en vertrouwensmodel

Dit model scheidt duidelijk de **uitgifte**, het **bewaren**, de **presentatie** en de **verificatie** van referenties, waardoor het tot stand brengen van vertrouwen, de controle en het hergebruik van referenties, contextuele beweringen en beleidsmatige handhaving onafhankelijk van elkaar worden afgehandeld.

Deze scheiding maakt schaalbare, interoperabele en controleerbare delegatie en autorisatie over organisatiegrenzen heen mogelijk.

Om interoperabiliteit tussen AORTA en Nuts (in beide richtingen) te ondersteunen, moet de identificatie van een zorgverlener expliciet worden opgesplitst in twee lagen:

- een **technische identificatiecode** (bijv. een DID) die uitsluitend wordt gebruikt voor het eigendom van cryptografische sleutels en bewijs van controle; en
- één of meer **verifieerbare referenties** die de gezaghebbende bedrijfsidentiteit uitdrukken, zoals URA, AGB, rol of mandaat.

Een technische identificatiecode MAG NIET op zichzelf worden gebruikt als identificatie van een zorgverlener.

Elke DID die in de PoC wordt gebruikt, MOET via een verifieerbare referentie, uitgegeven door een gezaghebbende bron, gekoppeld zijn aan ten minste één bedrijfsidentificatiecode die gelijkwaardig is aan die welke binnen AORTA worden gebruikt.

Een verifieerbare referentie die een dergelijke gezaghebbende DID-bedrijfsidentificatiecode-koppeling mist, MOET worden beschouwd als een onbeheerde claim en MAG NIET worden behandeld als een normatieve identiteit.

Verifiers MOGEN GEEN semantische betekenis toekennen aan een technische identificatiecode (DID) die verder gaat dan wat kan worden afgeleid uit gevalideerde verifieerbare referenties.

8.3.5 Rol van de GtK

De GtK biedt de noodzakelijke bemiddelingslaag om architectonische en vertrouwensmodelverschillen tussen domeinen op een gecontroleerde en controleerbare manier te overbruggen.

De GtK fungeert als een gestandaardiseerde toegangsinterface die:

- elk ecosysteem afschermt van de interne complexiteit van het andere,
- domeinspecifieke vertrouwens- en autorisatiebeleidsregels afdwingt, en
- waar nodig identificatoren, referenties en protocollen vertaalt.

De GtK fungeert als technische dienstverlener en KAN optreden als houder van verifieerbare referenties die zijn uitgegeven voor een zorgverlener, op basis van expliciete delegatie zoals gedefinieerd in hoofdstuk XXX.

Er bestaan twee afzonderlijke GtK's, elk afgestemd op het vertrouwensmodel en de governance van het betreffende domein.

8.3.5.1 GtK-Nuts

De GtK-Nuts interface communiceert met een of meer Nuts-nodes en:

- Biedt veilige inkomende en uitgaande communicatie voor deelnemers in het Nuts-ecosysteem.
- Interpreteert en handhaaft autorisatie op basis van:
  - Verifieerbare referenties,
  - DID-gebaseerde subjectidentificatie en
  - de attribuut- en delegatiemodellen die binnen Nuts zijn gedefinieerd.
- Fungeert als het beleidshandhavingspunt voor Nuts-verzoeken die de domeingrens overschrijden.

- Vertaalt externe verzoeken en antwoorden naar de juiste Nuts-protocollen, DID-referenties en FHIR-resources.

Vanuit het Nuts-perspectief is de GtK-Nuts een vertrouwde verifier en gateway die Nuts-interacties externaliseert zonder interne node-to-node vertrouwensmechanismen bloot te leggen.

8.3.5.2 GtK-AORTA

De GtK-AORTA biedt het gestandaardiseerde toegangspunt tot de LSP/AORTA-infrastructuur en:

- Valideert authenticatie- en autorisatiemetadata volgens de AORTA/LSP-vertrouwenskaders, waaronder:
  - X.509-certificaten,
  - UZI-gebaseerde identiteiten,
  - SAML-tokens of gelijkwaardige autorisatie-artefacten.
- Verifieert dat extern aangeboden referenties (inclusief VC's):
  - zijn uitgegeven door vertrouwde instanties,
  - correct zijn gekoppeld aan erkende bedrijfsidentificaties,
  - en voldoen aan het LSP-beleid en de reikwijdte van beperkingen.
- Zorgt voor consistente routering naar de juiste LSP-services, zoals:
  - medicatieservices,
  - professionele of patiëntendossierservices,
  - toestemmings- en registratieservices.

Vanuit het AORTA-perspectief zorgt de GtK-AORTA ervoor dat nieuwe referentiemodellen (VC's/DID's) kunnen worden gebruikt zonder de kernveronderstellingen van het LSP-vertrouwen te wijzigen.

8.3.6 End-to-end bridge architectuur

Door aan beide zijden een GtK te plaatsen, kunnen beide ecosystemen **onafhankelijk van elkaar** evolueren, terwijl een stabiele, controleerbare en veilige interface voor gegevensuitwisseling tussen domeinen behouden blijft.

De Nuts-LSP-brug bestaat daarom uit:

- een op verifieerbare referenties gebaseerd autorisatiemodel,
- op FHIR gebaseerde klinische datastructuren, en
- twee GtK's die de communicatiestromen tussen de twee vertrouwensdomeinen bemiddelen, valideren en converteren.

Deze aanpak zorgt ervoor dat vertrouwen, autorisatie en interoperabiliteit consistent blijven over het gehele end-to-end uitwisselingspad, ongeacht welk ecosysteem de interactie initieert.

8.3.7 Technische identificatoren en DID-methoden

Binnen de Nuts–LSP-brug worden gedecentraliseerde identificatoren (DID's) uitsluitend gebruikt als **technische identificatoren** voor het eigendom en de verificatie van cryptografische sleutels.

Een DID is een technische identificator die cryptografische controle door een entiteit vertegenwoordigt, maar op zichzelf geen juridische, organisatorische of autorisatiesemantiek overbrengt.

Bedrijfsidentiteit, rollen, mandaten en autorisaties worden uitgedrukt via verifieerbare referenties die zijn uitgegeven door gezaghebbende uitgevers.

Afhankelijk van de context kan een DID een zorgorganisatie vertegenwoordigen (bijv. cryptografisch gekoppeld aan een URA), een service (GtK) of een individuele gebruiker, waarbij de feitelijke betekenis en het vertrouwen ervan zijn afgeleid van de bijbehorende referenties.

De volgende DID-methoden worden in deze PoC gebruikt:

- **did:web**
  Deze methode koppelt een DID aan controle over een DNS-domein en een HTTPS-eindpunt. Het

wordt gebruikt om cryptografische sleutels aan een organisatie te koppelen op een manier die aansluit bij bestaande web- en operationele beveiligingspraktijken.

- **did:x509**
  Deze methode leidt een DID af van een bestaand X.509-certificaat of certificaatketen. Het maakt hergebruik mogelijk van bestaande PKI-vertrouwensankers, zoals UZI-certificaten, en ondersteunt een gecontroleerde overgang van certificaatgebaseerde identificatie (AORTA) naar op referenties gebaseerde autorisatie (Nuts).

DID-resolutie en sleutelvalidatie worden uitgevoerd door de GtK's om cryptografische controle te garanderen. Vertrouwensbeslissingen zijn gebaseerd op de validatie van verifieerbare referenties en hun **cryptografische koppeling** aan de **relevante DID's**, niet op de DID-methode zelf.

8.3.7.1 Metadata- en token-eindpunten

In het Nuts-LSP Proof of Concept worden metadata-eindpunten gebruikt om een **interoperabele** en **betrouwbare** uitwisseling van verifieerbare referenties (VC's) tussen deelnemende systemen mogelijk te maken.

Metadata biedt machineleesbare informatie over de technische mogelijkheden van een autorisatieserver of -uitgever, inclusief beschikbare token-eindpunten, ondersteunde authenticatiemechanismen, geaccepteerde VC- en VP-formaten en ondersteunde cryptografische algoritmen. Dit stelt partijen in staat om dynamisch te bepalen hoe ze met elkaar interageren, zonder afhankelijk te zijn van statische of bilaterale configuratie.

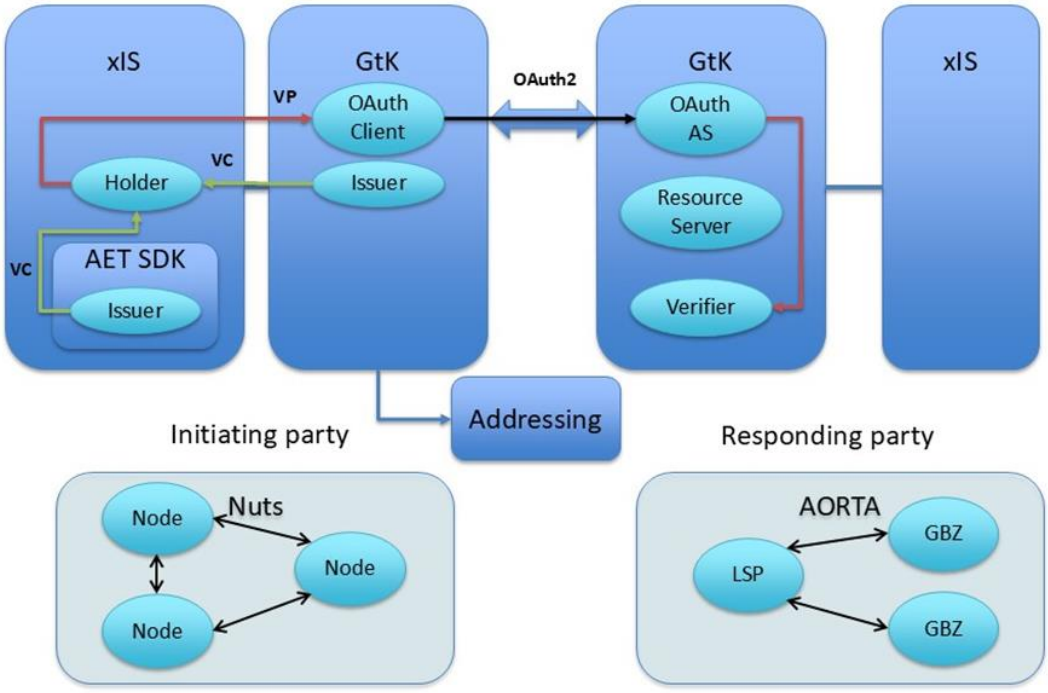
De PoC maakt gebruik van op OAuth 2.0 gebaseerde metadata, uitgebreid met VC-gerelateerde mogelijkheden zoals gedefinieerd in de OIDC4VC-specificatiefamilie. In deze opzet ondersteunen token-eindpunten **asymmetrische**, **certificaat**- of **sleutelgebaseerde authenticatie** (bijvoorbeeld JWT bearer grants), wat aansluit bij bestaande vertrouwensmodellen in de gezondheidszorg en systeem-naar-systeem en geautomatiseerde interacties mogelijk maakt.

Metadata speelt een cruciale rol in het gebruik van verifieerbare referenties door vooraf te definiëren welke referentieformaten, handtekeningen en identificatiemethoden worden geaccepteerd. Zonder deze informatie kan een referentie cryptografisch geldig zijn, maar toch incompatibel met het ontvangende systeem.

Binnen de Nuts-LSP-architectuur fungeren metadata-eindpunten als faciliterende vertrouwensinfrastructuur. Ze ondersteunen dynamische interoperabiliteit tussen Nuts-deelnemers en vormen de basis voor veilige VC-uitgifte en -verificatie, zonder onderdeel te worden van het zorgproces zelf.

8.4 Juridische uitgangspunten (was 6.5)

Credential flow and trust chain (diagram explanation)



The diagram is positioned primarily on the **application layer**, describing the technical credential, verification, and authorization flow between systems.
Actors such as healthcare providers, GtKs, and trust frameworks (e.g. Twiin) are treated as **business-layer roles** that are realized by application-layer components.

The healthcare provider remains the business subject of all business-related Verifiable Credentials, even when these credentials are held and presented by a delegated GtK (see Chapter 14).

The AET SDK is a **reusable application component** that may be embedded in systems participating at different points in the chain; it is not an actor in itself.

While the AET SDK is not an actor, it may technically perform credential issuance and signing functions on behalf of an issuing trust authority. In such cases, the SDK invokes a smartcard, HSM, or remote signing service to produce the cryptographic signature that is embedded in the issued Verifiable Credential. The issuer role and trust responsibility remain with the issuing authority, while the SDK acts as an implementation component realizing this function.

8.4.1 Defined interaction chain

The credential and authorization chain is defined as follows:

1. **Initiating xIS**
   Backend system of a healthcare provider acting as (logical) **holder** of business-related credentials.
2. **Initiating GtK**
   Acts as OAuth Client on behalf of the healthcare provider. The GtK acts as a technical service provider and may act as holder of Verifiable Credentials issued for a healthcare provider, based on explicit delegation as described in Chapter 14.
3. **Responding GtK**
   Acts in the roles of:
   a. OAuth Authorization Server

b. Verifier (of VPs and underlying VCs)
c. Resource Server

4. **Responding xIS**
   Backend system providing the protected healthcare service.

The **AET SDK** may be used by either an xIS or a GtK to support credential issuance, presentation, or verification, depending on the use case.

8.4.2 Credential issuance and binding

- Verifiable Credentials are issued under the authority of existing UZI trust anchors, including:
  - UZI server certificates
  - UZI personal certificates (UZI-card)

  The AET SDK may technically realize the credential issuance and signing process on behalf of the issuing trust authority, invoking a smartcard, HSM, or remote signing service.

- These Verifiable Credentials:
  - carry the **business identity, roles, and mandates** (e.g. healthcare provider, professional role, service authorization),
  - are cryptographically bound to a **DID** used as a technical identifier.
- The DID functions solely as a **cryptographic binding mechanism**; it does not replace or redefine the business identity expressed in the Verifiable Credentials.

8.4.3 Verifiable Presentation and OAuth flow

- For OAuth-based access:
  - A **Verifiable Presentation (VP)** is constructed and signed by the holder and passed to the **OAuth Client**, the **Initiating GtK**.
  - This VP is included in the OAuth token request (e.g. JWT bearer grant).
- The **Responding GtK**:
  - verifies the VP,
  - validates the included VCs,
  - evaluates them against Twiin trust, policy, and authorization rules,
  - and issues an **OAuth Access Token** if all conditions are met.

Applications use this access token to access protected resources via REST APIs.

8.4.4 Trust boundaries and qualified nodes

- Trust decisions are made exclusively by **qualified nodes**:
  - GtKs,
  - and other explicitly trusted VC issuers (e.g. Twiin, DEZI).
- All verification traffic (including VC and VP validation) is intended to occur **between GtKs**, shielding underlying xIS implementations from direct exposure.
- An xIS is only visible in the trust chain if:
  - it is explicitly defined as part of a GtK,
  - and included in the corresponding qualification and compliance scope.

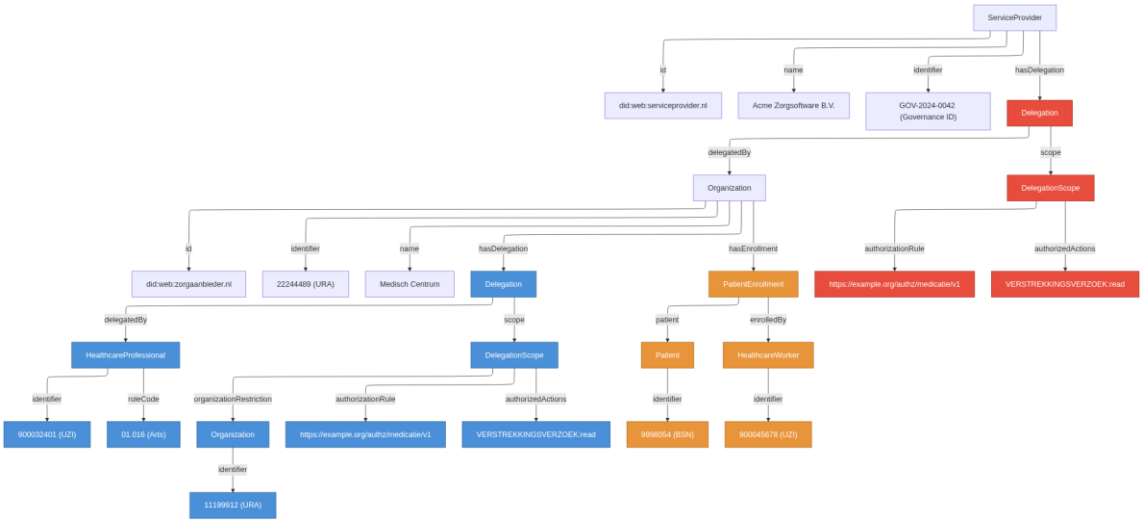
8.5 Objectives

- Ensure interoperability with existing holders, issuers, and verifiers.
- Avoid the creation of a proprietary “Nuts–LSP VC format” by aligning with recognized international standards.
- Preserve the authoritative role of existing registers and trust frameworks.
- Prepare for future implementations and evolutions, such as **DEZI**.

8.6 Ontologie: partijen, rollen en relaties

Dit onderdeel beschrijft de entiteiten, rollen en relaties die centraal staan in het geharmoniseerde model. Het dient als referentiemodel voor de rest van dit hoofdstuk en de technische specificaties in hoofdstuk 10. Het model is opgebouwd in drie lagen: de business-laag (wie zijn de partijen), de vertrouwenslaag (welke rollen spelen zij in het credential-model) en de technische laag (welke componenten zijn er).

// Ik weet niet waar deze thuishoort, maar bij deze even in de SOLL gezet ➔ Verplaatst van Soll naar 8.2



De ontologie beschrijft het domeinmodel met de entiteiten en relaties die worden geïdentificeerd en geverifieerd tijdens het authenticatieproces bij gegevensuitwisseling in de IST-situatie.

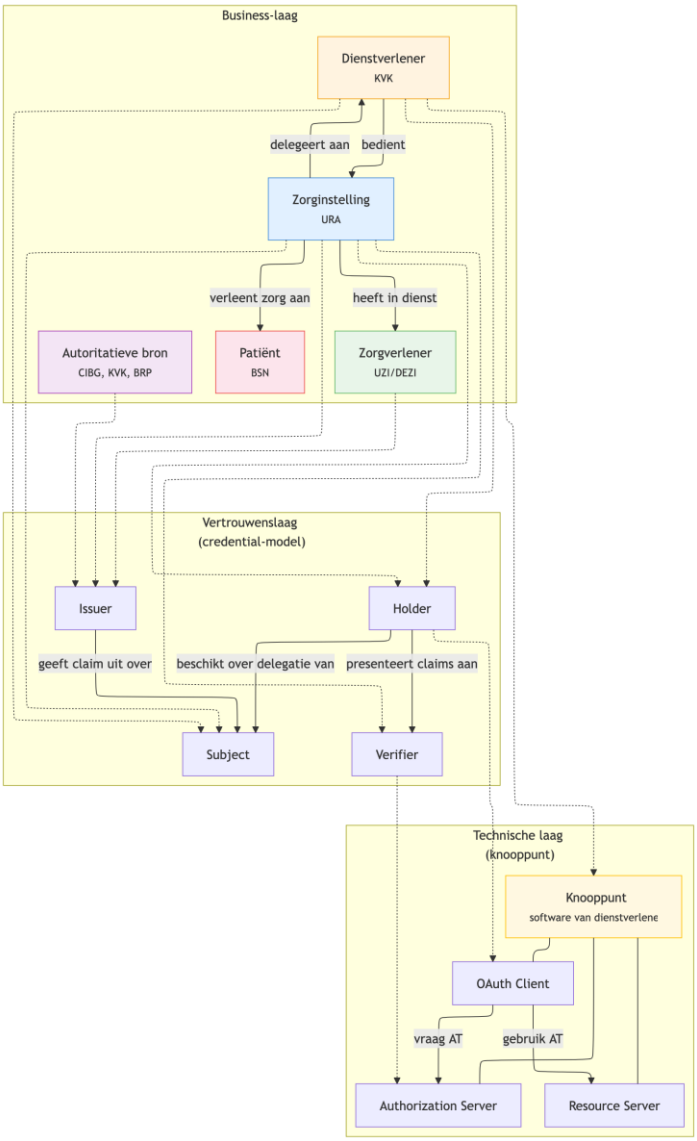
Centraal staan vijf entiteiten: **Organization** (zorgaanbieder), **HealthcareProfessional** (zorgverlener), **HealthcareWorker** (medewerker), **Patient** en **ServiceProvider** (softwareleverancier).

Zorgmedewerkers kunnen via een **Delegation** namens een zorgverlener handelen, waarbij een **DelegationScope** vastlegt welke autorisatieregels en acties zijn toegestaan. Patiëntinschrijvingen worden gemodelleerd als een expliciet **PatientEnrollment**-object, zodat vastgelegd wordt welke medewerker de inschrijving heeft uitgevoerd. Dezelfde delegatiestructuur wordt hergebruikt voor de mandatering van softwareleveranciers door zorgaanbieders zodat softwareleveranciers met de relatie t.o.v. de organisatie zichtbaar zijn in de transactie en kunnen handelen namens de organisatie.

De kleuren groeperen eigenschappen die samen over een entiteit worden beweerd.

- **Blauw** — de delegatie van zorgverlener aan organisatie (HealthcareProfessional, Delegation, DelegationScope met organizationRestriction)
- **Oranje** — de patiëntinschrijving (PatientEnrollment, Patient, HealthcareWorker)
- **Rood** — de delegatie van organisatie aan softwareleverancier (Delegation, DelegationScope vanuit ServiceProvider)

8.6.1 Overzicht



8.6.2 Business-laag

De business-laag beschrijft de partijen die deelnemen aan gegevensuitwisseling en hun onderlinge relaties.

Zorginstelling

De organisatie die verantwoordelijk is voor de zorgverlening en de gegevens van patiënten. Geïdentificeerd door een URA-nummer (IDENT-001). Een zorginstelling kan bevoegdheden delegeren aan een of meerdere dienstverleners (IDENT-010, IDENT-016), maar blijft altijd zelf verantwoordelijk (IDENT-013). Een zorginstelling kan ook haar eigen dienstverlener zijn; in dat geval vervult dezelfde organisatie beide rollen.

Dienstverlener

De partij die namens een zorginstelling handelt in het digitale domein. Geïdentificeerd door een KVK-nummer (IDENT-002). Een dienstverlener kan meerdere zorginstellingen bedienen (IDENT-011). De dienstverlener biedt een knooppunt aan waarmee de technische ontsluiting plaatsvindt.

Zorgverlener

De natuurlijke persoon die zorg verleent, in dienst van een zorginstelling. Geïdentificeerd door een UZI/DEZI-nummer (IDENT-003). In het authenticatiemodel ondertekent de zorgverlener niet zelf; de zorgverlener wordt vertegenwoordigd via de zorginstelling (AUTH-005).

Patiënt

De persoon die zorg ontvangt. Geïdentificeerd door het BSN (IDENT-004). Het BSN wordt waar nodig en mogelijk gepseudonimiseerd (IDENT-008).

Autoritatieve bron

Een register of instantie die verantwoordelijk is voor het uitgeven van identiteitsclaims over een specifiek attribuut (IDENT-007). Voorbeelden: CIBG (URA, UZI/DEZI), KVK (Handelsregister), BRP (BSN).

8.6.3 Vertrouwenslaag (credential-model)

De vertrouwenslaag beschrijft welke rollen de partijen uit de business-laag vervullen in het credential-model. Een partij kan meerdere rollen tegelijk vervullen.

Issuer

De partij die een verifieerbare claim uitgeeft over een subject. Autoritatieve bronnen (CIBG, KVK, BRP) zijn issuers van identiteitsclaims. Naast identiteitsclaims bestaan er ook relationele claims die iets zeggen over relaties tussen entitieten. Bijvoorbeeld, een zorginstelling is issuer een claim waarmee zij bevoegdheden delegeert aan een dienstverlener. Een behandelaar issued de claim over werken onder een rolcode en een zorgverlener issued claims over de behandelrelatie tussen een patiënt en een zorginstelling.

Subject

De partij waar een claim betrekking op heeft. De zorginstelling is doorgaans het subject van organisatie-gerelateerde claims (URA, organisatietype, certificeringen). De presenterende partij en het subject mogen verschillend zijn (IDENT-014).

Holder

De partij die claims beheert in een wallet. De zorginstelling is juridisch altijd holder van haar eigen claims en beheert haar eigen wallet (AUTH-025). Het operationele beheer van de wallet kan worden uitbesteed aan een dienstverlener. De dienstverlener kan via een expliciet delegatiebewijs namens de zorginstelling optreden en claims aanbieden aan een verifier (IDENT-022, AUTH-022). Voor de verifier maakt het niet uit wie het operationele beheer voert, mits de cryptografische validiteit en delegatiebewijzen correct zijn (AUTH-026).

Verifier

De partij die aangeboden claims controleert voordat zij toegang verleent tot beschermde gegevens. De verifier MOET het delegatiebewijs controleren (AUTH-021) en de intrekkingsstatus ervan kunnen vaststellen zonder synchrone calls naar de uitgever (AUTH-022). De verificatielogica is gebaseerd op cryptografische validiteit, niet op kennis van de interne organisatie van de presenterende partij (AUTH-026). De technische invulling van de verifier-rol vindt plaats in de Authorization Server en Resource Server van het knooppunt (zie Technische laag).

8.6.4 Technische laag (knooppunt)

De technische laag beschrijft de softwarecomponenten waarmee de rollen uit de vertrouwenslaag worden gerealiseerd.

Knooppunt

Het knooppunt is de software die door de dienstverlener wordt aangeboden en beheerd. Het knooppunt bevat de volgende OAuth-componenten:

OAuth Client: Het component dat namens de dienstverlener (en de zorginstelling waarvoor deze handelt) toegang vraagt tot beschermde gegevens bij een andere partij. De client presenteert claims en delegatiebewijzen in het token request (OAUTH-002, OAUTH-005).

Authorization Server (AS): Het component dat namens de bronhouder (zorginstelling) de identiteit en bevoegdheden van een inkomende client vaststelt en een access token uitgeeft. De AS is per URA adresseerbaar (OAUTH-008) en publiceert de delegatierelatie met de zorginstelling (OAUTH-013).

Resource Server (RS): Het component dat namens de bronhouder beschermde gegevens beheert en toegang verleent op basis van een geldig access token (OAUTH-015). Afhankelijk van het token type is er nog een introspectie bij de AS nodig.

Een knooppunt kan namens meerdere zorginstellingen opereren (multi-tenant, OAUTH-012). Het LSP-Gtk en Nuts-nodes zijn beide voorbeelden van knooppunten; zij verschillen in architectuur (centraal vs. decentraal) maar vervullen dezelfde rollen. De bedoeling is dat de technische werking van deze knooppunten wordt gestandaardiseerd in landelijke afspraken.

8.7 Identiteitsmodel

8.7.1 DID-methode en identifier-strategie

Elke deelnemer in het stelsel heeft een technische identifier nodig die herleidbaar is naar sleutelmateriaal (AUTH-011), maar gescheiden is van business identifiers zoals URA en KVK (AUTH-012). Hiervoor wordt gebruik gemaakt van Decentralized Identifiers (DIDs). Een DID is een globally unieke identifier die de eigenaar zelf beheert en die resolveert naar een DID-document met daarin het publieke sleutelmateriaal van die partij.

In het geharmoniseerde model worden twee DID-methoden ingezet, elk met een eigen rol:

did:web is de primaire DID-methode voor deelnemers aan het stelsel. Een did:web identifier is gekoppeld aan een webdomein dat de deelnemer beheert (bv. did:web:example-ziekenhuis.nl). Het bijbehorende DID-document wordt gepubliceerd op een well-known URL onder dat domein en bevat het publieke sleutelmateriaal van de deelnemer. did:web ondersteunt sleutelrotatie zonder wijziging van de identifier (AUTH-017), meerdere sleutels voor verschillende doeleinden (AUTH-015), en is vindbaar zonder centrale infrastructuur. Dienstverleners en zorginstellingen gebruiken did:web als hun technische identifier voor het ondertekenen van presentaties, het uitgeven van DelegationVCs.

did:x509 wordt ingezet als brug naar de bestaande X.509 certificaatinfrastructuur. Deze methode maakt het mogelijk om attributen uit een X.509 certificaat (zoals een URA-nummer of organisatienaam) te gebruiken als basis voor het uitgeven van Verifiable Credentials. De did:x509 identifier is afgeleid van eigenschappen in de certificaatketen en kan door een verifier lokaal geresolveerd worden op basis van de meegeleverde certificaatketen. Dit is met name relevant voor autoritatieve bronnen die al over X.509 certificaten beschikken (bv. via PKIoverheid) en hiermee VCs kunnen uitgeven over organisaties in het stelsel. Zo wordt voldaan aan AUTH-006: het stelsel kan flexibel omgaan met zowel de huidige generatie certificaten als toekomstige identificatiemiddelen.

De combinatie van beide methoden zorgt ervoor dat het stelsel voortbouwt op de bestaande PKI-infrastructuur (AUTH-006) zonder er volledig van afhankelijk te zijn, en dat nieuwe deelnemers kunnen toetreden met een lichtgewicht DID-methode.

8.7.2 Credential structuur

Het geharmoniseerde model kent een beperkte set Verifiable Credentials waarmee de identiteit van partijen en hun onderlinge relaties worden vastgelegd. Elk credential heeft een specifiek doel en een duidelijke issuer-subject relatie. De credentials zijn onderverdeeld in identificerende credentials (wie ben je?) en delegatie-credentials (namens wie mag je handelen?).

Identificerende credentials

HealthcareProviderCredential Uitgegeven via did:x509 op basis van een certificaat dat het URA-nummer van de zorginstelling bevat. Dit credential bewijst de identiteit van de zorginstelling als erkende zorgaanbieder. Het vormt de basis waarop delegaties worden gebouwd: zonder een geldig HealthcareOrganizationCredential kan een zorginstelling geen delegaties uitgeven.

- Issuer: autoritatieve bron (via did:x509, certificaatketen)
- Subject: zorginstelling (did:web)
- Belangrijkste claims: URA-nummer, organisatienaam

ServiceProviderCredential Uitgegeven door een stelselhouder, bevat de identiteit van de dienstverlener en de diensten die de dienstverlener mag leveren binnen het stelsel. Dit credential geeft de OAuth client de autorisatie om verbinding te mogen maken met een authorization server. Het fungeert als bewijs dat de dienstverlener is toegelaten tot het stelsel.

- Issuer: stelselhouder
- Subject: dienstverlener (did:web)
- Belangrijkste claims: KVK-nummer, naam dienstverlener, stelseltoelating, lijst van toegestane diensten

Opmerking: momenteel is er nog geen operationele stelselhouder die dit credential kan uitgeven. Als tijdelijke oplossing kunnen certificaten van een hoog vertrouwensniveau (bv. PKIoverheid) worden gebruikt, eventueel aangevuld met een allow-list tijdens kleinschalige pilots.

Relationele credentials

PatientEnrollmentCredential Uitgegeven via did:x509, bedoeld om de inschrijving van een patiënt bij een zorginstelling aantoonbaar te maken. Dit credential maakt het mogelijk om het access token te binden aan een specifieke patiënt, zodat de bronhouder kan vaststellen dat de raadplegende partij een actieve behandelovereenkomst heeft met de betreffende patiënt.

- Issuer: autoritatieve bron (via did:x509, certificaatketen)
- Subject: zorginstelling (did:web)
- Belangrijkste claims: patiëntidentificatie (BSN, optioneel gepseudonimiseerd), zorginstelling (URA)

HealthcareProfessionalDelegationCredential Dit credential legt vast dat een zorgverlener met een UZI-registratie (en bijbehorende rolcode) de verantwoordelijkheid voor specifieke handelingen delegeert aan een afdeling of organisatie. Hierdoor kan de organisatie namens deze behandelaar handelen zonder dat de zorgverlener zelf bij elke transactie hoeft te authenticeren (AUTH-005). Dit is essentieel voor de gebruiksvriendelijkheid in het klinische werkproces.

Dit credential wordt altijd uitgegeven aan de eigen werkgever van de zorgverlener. De werkrelatie tussen zorgverlener en zorginstelling is niet technisch verifieerbaar uit het UZI-certificaat; en leiden we af uit het bestaan en bezit van het credential door de zorginstelling.

- Issuer: zorgverlener (via did:x509, UZI-certificaat)
- Subject: zorginstelling of afdeling (did:web)
- Belangrijkste claims: UZI-nummer uit het UZI pas certificaat, rolcode, scope van de delegatie

ServiceProviderDelegationCredential Dit credential maakt de delegatie van de zorginstelling naar de dienstverlener expliciet (IDENT-023, IDENT-024). Het legt vast dat de dienstverlener handelingsbevoegdheid heeft namens de zorginstelling, gescoped tot specifieke diensten of toepassingen (IDENT-015). De scope in dit credential bevat een set of subset van de diensten die zijn opgenomen in het ServiceProviderCredential van de dienstverlener. Dit is het credential dat de verifier controleert voordat hij claims of beschermde gegevens accepteert (AUTH-021).

- Issuer: zorginstelling (via did:web)
- Subject: dienstverlener (did:web)
- Belangrijkste claims: zorginstelling (URA), dienstverlener (KVK-nummer), scope (diensten/toepassingen), geldigheidsperiode

Overzicht

Credential	Type	Issuer	Subject	Doel
HealthcareProviderCredential	Identificerend	UZI Server certificaat (did:x509)	Zorginstelling (did:web)	Identiteit van de zorginstelling
ServiceProvider-Credential	Identificerend	Stelselhouder	Dienstverlener (did:web)	Toelating dienstverlener tot het stelsel
PatientEnrollment-Credential	Relatie	Medewerker (did:x509)	Zorginstelling (did:web)	Aantonen behandelrelatie met patiënt
HealthcareProfessional-DelegationCredential	Relatie	Zorgverlener (did:x509)	Zorginstelling (did:web)	Handelen namens behandelaar zonder per-transactie authenticatie
ServiceProviderDelegationCredential	Relatie	Zorginstelling (did:web)	Dienstverlener (did:web)	Handelingsbevoegdheid dienstverlener namens zorginstelling

Relatie tussen credentials

De credentials vormen samen een vertrouwensketen:

1. De **HealthcareProviderCredential** bewijst de identiteit van de zorginstelling
2. De **ServiceProviderCredential** bewijst de toelating van de dienstverlener tot het stelsel en definieert welke diensten deze mag leveren
3. De **ServiceProviderDelegationCredential** verbindt deze twee: de zorginstelling delegeert specifieke bevoegdheden aan de dienstverlener, gescoped tot een subset van de diensten uit het ServiceProviderCredential
4. De **HealthcareProfessionalDelegationCredential** voegt de zorgverlener-context toe: een behandelaar delegeert verantwoordelijkheid aan de organisatie
5. De **PatientEnrollmentCredential** bindt de transactie aan een specifieke patiënt

8.8 Presentatie en verificatie

8.8.1 Presentatie-model

In het geharmoniseerde model presenteert de dienstverlener (als OAuth client) twee Verifiable Presentations in het token request, met daarin VCs gegroepeerd op subject en ondertekend onder controle van het subject:

VP 1: Zorginstelling Bevat alle credentials die betrekking hebben op de zorginstelling als subject:

- HealthcareProviderCredential (identiteit)
- PatientEnrollmentCredential (behandelrelatie)
- HealthcareProfessionalDelegationCredential (mandaat van behandelaar)

VP 2: Dienstverlener Bevat alle credentials die betrekking hebben op de dienstverlener als subject:

- ServiceProviderCredential (stelseltoelating)
- ServiceProviderDelegationCredential (delegatie van zorginstelling)

De keuze voor twee VPs volgt uit AUTH-020: claims in een enkele presentatie moeten altijd betrekking hebben op hetzelfde subject. Door te groeperen op subject wordt het standaard VP-model gevolgd, waarbij de issuer van de VP (de ondertekenaar) overeenkomt met het subject van de ingesloten credentials. Dit voorkomt niet-standaard business rules bij de verificatie.

De twee VPs samen bieden de verifier in één transactie alle informatie die nodig is om vast te stellen wie de handeling uitvoert (dienstverlener), namens wie (zorginstelling), op basis van welk mandaat (delegatie), voor welke patiënt (enrollment) en met welke professionele verantwoordelijkheid (behandelaar).

8.8.2 VC Repository architectuur

De zorginstelling is juridisch altijd eigenaar van haar eigen repository (AUTH-025). Het operationele beheer kan worden uitbesteed aan de dienstverlener. Voor de verifier maakt dit geen verschil: de verificatie is gebaseerd op cryptografische validiteit en correcte delegatiebewijzen, niet op kennis van wie de repository operationeel beheert (AUTH-026).

In de huidige situatie zal de dienstverlener in veel gevallen het operationele beheer van de repository van de zorginstelling op zich nemen. Dit is een pragmatische startsituatie, maar niet de gewenste eindsituatie. Naarmate het stelsel volwassener wordt, is het wenselijk dat zorginstellingen hun eigen repository beheren. Dit wordt met name relevant wanneer een zorginstelling met meerdere dienstverleners werkt (IDENT-016): een eigen repository voorkomt dat credentials en sleutelmateriaal bij meerdere dienstverleners moeten worden beheerd of gedupliceerd. De zorginstelling beheert dan centraal haar eigen identiteit en geeft aan elke dienstverlener een ServiceProviderDelegationCredential met de juiste scope.

Ongeacht wie het operationele beheer voert: VP 1 (zorginstelling) wordt altijd ondertekend met sleutelmateriaal van de zorginstelling, VP 2 (dienstverlener) met sleutelmateriaal van de dienstverlener (AUTH-015).

8.8.3 Verificatieproces

De verifier (authorization server van de bronhouder) voert de volgende controles uit op de vertrouwensketen uit de claims bij ontvangst van een token request:

1. **Stelseltoelating**: is de dienstverlener toegelaten tot het stelsel? (ServiceProviderCredential)

2. **Delegatie**: heeft de dienstverlener handelingsbevoegdheid namens de zorginstelling, en valt de gevraagde dienst binnen de scope? (ServiceProviderDelegationCredential)
3. **Identiteit zorginstelling**: is de zorginstelling een erkende zorgaanbieder? (HealthcareProviderCredential)
4. **Behandelrelatie**: heeft de zorginstelling een behandelrelatie met de betreffende patiënt? (PatientEnrollmentCredential)
5. **Professionele verantwoordelijkheid**: is er een mandaat van een behandelaar met de juiste rolcode? (HealthcareProfessionalDelegationCredential)

De volgorde is bewust zo gekozen dat de meest gevoelige informatie (patiëntidentificatie) pas wordt geaccepteerd nadat de identiteit en bevoegdheid van de raadplegende partij is vastgesteld (AUTH-021, AUTH-024).

8.9 OAuth-profiel

8.9.1 Overzicht

Het OAuth-profiel implementeert de authenticatie-requirements door het token request te gebruiken als het moment waarop de dienstverlener alle benodigde claims en delegatiebewijzen presenteert aan de authorization server van de bronhouder. Het profiel is gebaseerd op RFC 7523 (JSON Web Token Profile for OAuth 2.0 Client Authentication and Authorization Grants), uitgebreid met Verifiable Presentations.

Het token request bevat twee aspecten:

- **Client authenticatie**: de VP met claims waar de dienstverlener zich identificeert en authenticeert als OAuth client
- **Authorization grant**: de VP met claims over de zorginstelling worden gepresenteerd als authorization grant conform RFC 7523

Hiermee wordt het onderscheid tussen de partij die het token aanvraagt (client/dienstverlener) en de partij namens wie toegang wordt gevraagd (subject/zorginstelling) expliciet gemaakt (OAUTH-006).

8.9.2 Token request flow

De token request flow verloopt als volgt:

1. De client (knooppunt van de dienstverlener) resolveert het token endpoint van de authorization server via de Care Services Directory, op basis van de URA van de bronhouder en het gewenste type gegevensuitwisseling (ADR-004)
2. De client stelt twee VPs samen zoals beschreven in sectie 8.4.1
3. De client stuurt een token request naar het token endpoint, met daarin:
    a. VP 1 (zorginstelling) als authorization grant
    b. VP 2 (dienstverlener) als client assertion
    c. De gewenste scope
    d. Een DPoP proof (zie 8.5.4)
4. De authorization server voert het verificatieproces uit zoals beschreven in sectie 8.4.3
5. Bij succesvolle verificatie geeft de AS een access token uit, gebonden aan de URA van de bronhouder (OAUTH-008) en aan de DPoP-sleutel van de client (OAUTH-010)
6. De client gebruikt het access token bij de resource server, vergezeld van een verse DPoP proof

Dit is een volledig back-channel flow zonder user-agent redirect (OAUTH-004), wat past bij zowel door gebruikers geinitieerde als geautomatiseerde interacties (AUTH-004).

8.9.3 Multi-tenancy en AS-discovery

Een dienstverlener kan namens meerdere zorginstellingen een authorization server draaien (OAUTH-012). Elke zorginstelling waarvoor de AS opereert wordt geïdentificeerd door een eigen unieke identifier. De vorm van deze identifier volgt de specificatie van RFC 8414 sectie 2 en is een URL. De inhoud is voor de client betekenisloos. (een client kan geen aannames doen over de vorm het bestaan van een identifier). Een manier om de issuer identifier uniek per zorginstelling te nummeren kan worden bereikt door het opnemen van een pad element met bijvoorbeeld een URA.

Een client dient zelf via een vertrouwde route de juiste AS identifier op te zoeken in bijvoorbeeld een adresseringsfunctie of een vooral geconfigureerde tabel.

De AS-metadata wordt gepubliceerd conform RFC 8414. Bijvoorbeeld:

Een dienstverlener beheert de AS voor een zorginstelling met URA 12345678. De issuer identifier voor deze zorginstelling is:

```
https://as.dienstverlener.nl/ura/12345678
```

Conform RFC 8414 wordt het metadata-document gevonden door /.well-known/oauth-authorization-server in te voegen tussen het host-deel en het pad-deel van de issuer identifier:

```
https://as.dienstverlener.nl/.well-known/oauth-authorization-
server/ura/12345678
```

Dit metadata-document bevat onder andere het token endpoint voor deze specifieke zorginstelling, bv.:

```
{
  "issuer": "https://as.dienstverlener.nl/ura/12345678",
  "token_endpoint": "https://as.dienstverlener.nl/oauth2/token",
  "grant_types_supported": [...],
  "scopes_supported": [...],
  ...
}
```

Merk op dat het token endpoint niet zorginstelling specifiek hoeft te zijn, gezien dit door het endopint kan worden afgeleid uit de audience van de meegestuurde assertions welke de AS identifier van de zorginstelling moeten bevatten.

8.9.4 Token binding (DPoP)

Access tokens worden gebonden aan het sleutelmateriaal van de client via het DPoP-mechanisme (Demonstrating Proof-of-Possession, RFC 9449). Bij elk gebruik van het access token stuurt de client een verse DPoP proof mee, ondertekend met dezelfde sleutel waarmee het token werd aangevraagd. Dit voorkomt dat gestolen tokens door andere partijen kunnen worden gebruikt (OAUTH-010).

8.9.5 Scope en toegangscontrole

De scope in het token request bepaalt welk type gegevensuitwisseling wordt gevraagd. De authorization server controleert of de gevraagde scope past binnen:

- De diensten die de dienstverlener mag leveren (ServiceProviderCredential)
- De bevoegdheden die de zorginstelling aan de dienstverlener heeft gedelegeerd (ServiceProviderDelegationCredential)

- De rolcode van de behandelaar (HealthcareProfessionalDelegationCredential)

Scope-gebaseerde toegangscontrole is afgestemd op bestaande zorg-OAuth-profielen zoals SMART-on-FHIR (OAUTH-009).

8.10 Sleutelmateriaal en PKI

8.10.1 PKI-architectuur

Het geharmoniseerde model maakt gebruik van twee lagen van publieke sleutelinfrastructuur:

X.509 certificaten vormen de basis voor de **did:x509** methode en voor de TLS-beveiliging van **did:web endpoints**. Voor TLS wordt gebruik gemaakt van certificaten uit het **PKIoverheid-stelsel**. Op termijn is de verwachting dat er een nieuwe certificaattak wordt ingericht binnen het **GIS-VN (Gezondheidsinformatie Stelsel Veilig Netwerk)**, specifiek voor deelnemers aan het gezondheidsinformatiestelsel. Tot die tijd worden PKIoverheid-certificaten of certificaten van vergelijkbaar vertrouwensniveau gebruikt.

DID-documenten bevatten het **publieke sleutelmateriaal** waarmee VCs en VPs worden ondertekend en geverifieerd. Voor **did:web** wordt het DID-document gepubliceerd op het domein van de deelnemer, beveiligd met TLS op basis van bovengenoemde certificaten. Voor **did:x509** wordt het sleutelmateriaal afgeleid uit de certificaatketen zelf.

De combinatie zorgt ervoor dat het vertrouwen in **did:web** uiteindelijk is verankerd in de PKI-infrastructuur (via TLS), terwijl **did:x509** direct op de bestaande certificaatinfrastructuur voortbouwt.

8.10.2 Sleutelbeheer

Elke deelnemer beheert meerdere sleutels voor verschillende doeleinden (AUTH-015). In de praktijk betekent dit minimaal:

- **Credential Signing key voor VCs**: gebruikt door issuers (zorginstellingen, autoritatieve bronnen) om credentials te ondertekenen. Deze sleutels hebben de hoogste vertrouwenseisen omdat de claims die ermee worden ondertekend langdurig geldig kunnen zijn.
- **Presentation Signing key voor VPs**: gebruikt door holders (zorginstellingen, dienstverleners) om presentaties te ondertekenen. Deze sleutels worden gebruikt bij elke transactie en hebben een korter risicoprofiel.
- **DPoP Signing key**: gebruikt door de OAuth client om token binding te realiseren. Deze sleutel is gebonden aan de sessie of het knooppunt.

De scheiding tussen deze sleutels voorkomt dat compromittering van een transactiesleutel automatisch leidt tot het kunnen uitgeven van valse credentials (AUTH-015).

8.10.3 Sleutelrotatie en intrekking

Sleutelrotatie wordt ondersteund via het **DID-document**: een deelnemer kan sleutelmateriaal toevoegen en verwijderen zonder dat de DID zelf wijzigt (AUTH-017). Verifiers resolven het DID-document om actueel sleutelmateriaal op te halen.

Voor **intrekking** van credentials en delegatiebewijzen wordt een mechanisme gehanteerd waarmee verifiers de intrekkingsstatus offline of via een gedeeld register kunnen controleren, zonder synchrone calls naar de uitgever (AUTH-022, OAUTH-016). De exacte keuze voor een revocation-mechanisme wordt uitgewerkt in de technische specificaties (hoofdstuk 10).

8.10.4 Open punten

De eisen aan de beveiliging van sleutelmateriaal zijn niet voor alle sleutels gelijk. Signing keys voor langlopende credentials hebben een fundamenteel ander risicoprofiel dan sleutels voor kortdurende presentaties of DPoP proofs. De volgende vragen staan nog open:

1. **Hardware-gebaseerde sleutelopslag**. In hoeverre hardware-gebaseerde sleutelopslag (HSM, secure enclave) vereist is, en hoe dit zich verhoudt tot de toetredingsdrempel voor met name de VVT-sector (OV-009)
2. **Sterke gebruikersauthenticatie**. Of sterke gebruikersauthenticatie voor sleutelgebruik vereist is bij geautomatiseerde systemen (OV-010)
3. **Vertrouwensniveaus.** Of er vertrouwensniveaus gedefinieerd moeten worden met per niveau verschillende eisen aan sleutelbeheer, opslag en intrekking (OV-011)

8.11 Adressering

LET OP: Hevig in flux!
De landelijke generieke functie voor adressering is gebaseerd op het IHE Mobile Care Services Directory (mCSD), zoals uitgewerkt in de Generieke Functies specificatie. In het geharmoniseerde model moeten systemen de technische endpoints kunnen vinden waarmee systemen van zorgaanbieders bereikbaar zijn.

~~partijen uit beide netwerken elkaars endpoints kunnen vinden op basis van een URA-nummer en een toepassing of datatype, ongeacht achter welk knooppunt deze endpoints zich bevinden (ADR-004).~~

8.11.1 Topologie

De Care Services Directory kent een gedistribueerde opzet met meerdere Administration Directories die worden geaggregeerd in Query Directories:

- **Nuts-knooppunten** fungeren elk als een eigen Administration Directory en Query Directory. Elk Nuts-knooppunt publiceert de endpoints van de zorginstellingen waarvoor het opereert en aggregeert de directories van andere knooppunten.
- **Het LSP** registreert endpoints van haar achterliggende systemen in ~~namens haar achterliggende systemen in een centrale Administration Directory, waarschijnlijk~~ ZORG-AB. Achterliggende partijen hoeven hier zelf geen actie voor te ondernemen (ADR-002, HAR-010).
- Het **Landelijk Register Zorgaanbieders** (LRZa) fungeert als **root Administration Directory** of registry. Iedere zorginstelling registreert bij het LRZa het endpoint van haar eigen Administration Directory. Update Clients kunnen het LRZa raadplegen om alle Administration Directories te ontdekken en deze gegevens te consolideren in Query Directories, waarmee een landelijke vindbaarheid en consistentie van endpoints wordt gewaarborgd.

8.11.2 Publicaties van endpoints

Endpoints worden gepubliceerd door het knooppunt dat de technische toegang tot een zorgaanbieder verzorgt. Het knooppunt publiceert deze endpoints namens de aangesloten zorginstellingen in de Care Services Directory.

8.11.3 Vindbaarheid van endpoints

Een zoekend systeem vindt het juiste endpoint via de volgende stappen:

1. Zoek in de Query Directory naar de organisatie op basis van het URA-nummer
2. Filter de beschikbare HealthcareServices op het gewenste type dienst of gegevensuitwisseling.
3. Selecteer het juiste Endpoint op basis van het payload type (ADR-007)

Omdat een zorgaanbieder via meerdere knooppunten bereikbaar kan zijn (bv. zowel via het LSP als via een Nuts-knooppunt), kan de Query Directory meerdere endpoints voor dezelfde combinatie van URA en diensttype bevatten. De exacte routeringslogica voor dit scenario is een open onderzoeksvraag (OV-007).

8.11.4 Relatie met OAuth-discovery

De Care Services Directory bevat naast de resource server endpoints ook de OAuth endpoints (authorization server, token endpoint) van elk knooppunt. Via de Endpoint-resources in de directory kan een zoekend systeem de issuer identifier van de authorization server vinden voor een specifieke URA, en daaruit het .well-known/oauth-authorization-server metadata-document resolven (zie 8.5.3). Hierdoor vormen adressering en authenticatie samen een sluitende keten:

URA → endpoint → AS-metadata → token request

8.11.5 Vertrouwen in registraties

De relatie tussen een knooppunt en de zorginstellingen waarvoor het endpoints publiceert moet verifieerbaar zijn (ADR-005). Dit wordt geborgd doordat:

- Het LRZa alleen registraties accepteert van zorginstellingen die hun eigen Administration Directory endpoint hebben vastgelegd
- Een Administration Directory alleen autoritatief is voor de zorginstellingen die er expliciet aan zijn gekoppeld via het LRZa
- De delegatierelatie tussen zorginstelling en dienstverlener cryptografisch verifieerbaar is via het ServiceProviderDelegationCredential (zie 8.3.2)

8.12 Lokalisatie

De lokalisatiefunctie stelt zorgverleners in staat om te ontdekken welke organisaties relevante patiëntgegevens van een bepaald type beschikbaar hebben. De landelijke voorziening hiervoor is de Nationale Verwijs Index (NVI). In het geharmoniseerde model moeten partijen uit beide netwerken lokalisatierecords kunnen registreren en bevragen bij de NVI (LOK-001, LOK-002).

8.12.1 Deelname aan de NVI

Zowel partijen aangesloten via het LSP als via Nuts-knooppunten nemen deel aan de NVI:

- **Het LSP** registreert en beheert lokalisatierecords namens haar achterliggende systemen, zonder dat die systemen hier zelf actie voor hoeven te ondernemen (LOK-003). Dit is consistent met de rol van het LSP als knooppunt (HAR-010).
- **Nuts-knooppunten** registreren lokalisatierecords voor de zorginstellingen waarvoor zij opereren. Elke zorginstelling is via haar knooppunt zelfstandig verantwoordelijk voor de juistheid van haar registraties.

8.12.2 Pseudonimisering

De NVI werkt met gepseudonimiseerde patiëntidentificatie om te voorkomen dat het BSN direct wordt uitgewisseld en de NVI een privacy hot-spot wordt. Partijen uit beide netwerken moeten toegang hebben tot de VWS pseudonimiseringsdienst (PRS) om lokalisatierecords te kunnen registreren en bevragen (LOK-005).

8.12.3 Authenticatie met de NVI en PRS

De NVI stelt eisen aan de identiteit van de bevragende partij, waaronder organisatie-identifier (URA), organisatietype, en mogelijk de identificatie van de zorgverlener (UZI/DEZI) en rolcode. De authenticatie tussen deelnemers en de NVI volgt een eigen mechaniek die wordt vastgesteld door VWS en niet noodzakelijk overeenkomt met het OAuth-profiel zoals beschreven in sectie 8.5.

De exacte authenticatie-eisen en -mechaniek voor de interactie met de NVI vallen buiten de scope van dit document. Hiervoor wordt verwezen naar de documentatie van VWS over de Generieke Functie Lokalisatie. Wel is het van belang dat de identiteitsattributen die de NVI vereist afleidbaar zijn uit het geharmoniseerde authenticatiemodel (LOK-004). Voor partijen die niet over een UZI-pas beschikken (met name in de VVT-sector) is dit nog een openstaand punt (OV-008).

Een specifiek aandachtspunt is het "device-id" dat VWS heeft geïntroduceerd voor de Generieke Functies. Dit is een identiteitsattribuut dat een combinatie van dienstverlener en zorginstelling vertegenwoordigt. Het device-id wordt tijdens authenticatie aangetoond en geeft de client autorisatie voor administratieve handelingen (aanmaken, opvragen en verwijderen) van lokalisatierecords die aan dat device-id zijn gekoppeld. Dit identiteitsattribuut bestaat uitsluitend binnen de VWS Generieke Functies en komt niet voor in het credential-model zoals beschreven in sectie 8.3.2. De wijze waarop het device-id wordt afgeleid uit of gemapt op de identiteitsattributen van het geharmoniseerde model (met name de combinatie van ServiceProviderCredential en HealthcareProviderCredential) vereist nadere uitwerking.

8.12.4 Toestemmingsmodel

Het is nog niet definitief vastgesteld of toestemming van de patiënt vereist is voordat lokalisatiegegevens worden gedeeld met een zoekende organisatie. Dit heeft directe gevolgen voor de oplossing:

- Indien toestemming vereist is, moet de NVI bij elke bevraging een consent-check kunnen uitvoeren richting de bronhouder (LOK-006). Dit vereist dat de identiteitsattributen van de zoekende partij voldoende zijn om deze check uit te voeren.
- Indien geen toestemming vereist is, kan de NVI volstaan met het verifiëren van de identiteit en bevoegdheid van de zoekende partij zonder een consent-check bij de bronhouder.

De keuze hierin wordt bepaald door VWS en valt buiten de scope van dit document. De gekozen oplossingsrichting voor het geharmoniseerde model moet beide scenario's kunnen accommoderen.

8.13 Beantwoording onderzoeksvragen

8.14 Route 1: Nuts bevraagt LSP

Deze routes in een los hoofdstuk zetten?

8.14.1 High-level flow

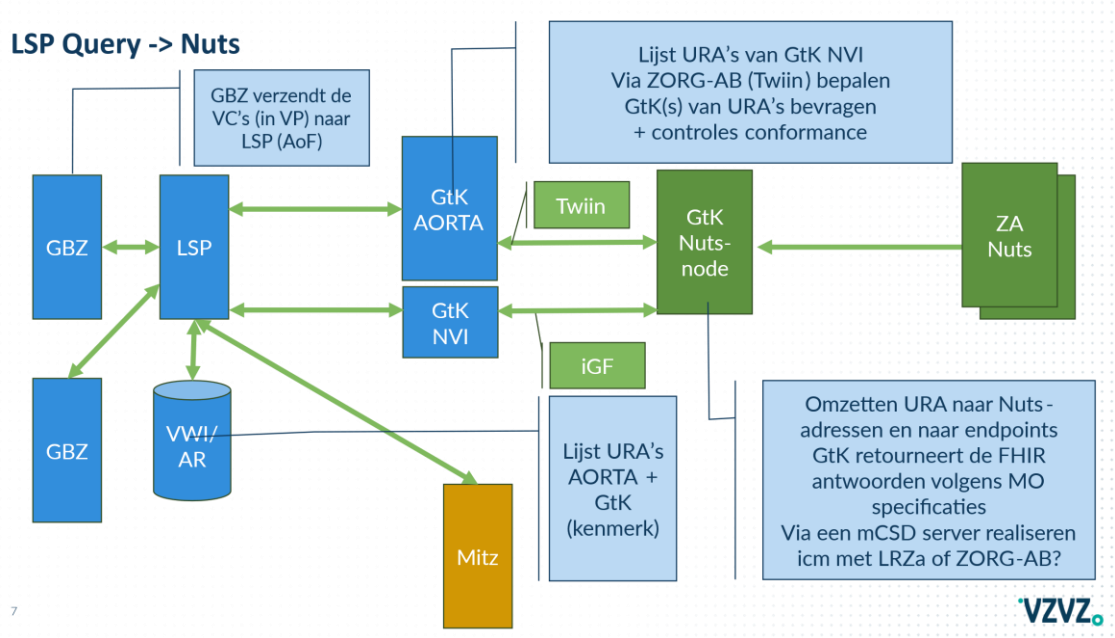
8.15 Route 2: LSP bevraagt Nuts

Doelstelling is om vanuit AORTA Nuts te kunnen bevragen zonder verschil te behoeven te maken of de bevraagde zorgaanbieder nu een AORTA-deelnemer is of een Nuts deelnemer.

Uitgangspunt is dat het 'vragende' systeem dan wel overstapt op de VC's, die we gezamenlijk hebben vastgesteld. De VC's worden immers ook bruikbaar voor het eigen AORTA-verkeer. 'Vertalen' van SAML2-tokens naar VC's is niet mogelijk gezien de cryptografische borging van de VC's. Dit gaan omzetten middels een 'vertaler' is, net zoals we dat bij Nuts hebben gedaan, niet mogelijk.

Er is dus **impact** voor AORTA-deelnemers als zij ook buiten AORTA willen kunnen raadplegen.

Omdat het LSP ook de lokalisatie uitvoert voor de AORTA-deelnemers en de adressering van de aangesloten zorgaanbieders transparant heeft gemaakt middels 'AppID's' zal er een route moeten worden bepaald waarlangs de bevragingen lopen:



Omdat er nog geen landelijk beschikbare NVI is wordt er een interface van de NVI gebouwd (GtK NVI). Deze stopt de entries in

8.15.1 <oplossingsrichting>

8.16 Risico's en mitigaties

Kwetsbaarheid	kans	impact	risico	oplossing
				<nr met kruis-verwijzing>

BIA, PIA, DPIA?

9 Fasering van de oplossingen

9.1 Pilot 1

Nuts vraagt gegevens op bij een LSP partij.

Beschrijf hier hoe de architectuur exact er uit komt te zien aan de kant van Nuts en van het LSP:

Waar staan de organisatie VC Repo's? Hoe komen de VCs uit de org-VC-repo bij de SP client terecht?

Wat komt er in de services van de delegationCredential terecht?

Wie is tijdens de pilots de stelselbeheerder en bepaalt wie er mee doet in de pilots en stelt dus vast wie een servivce provider is. En dan ook hoe identificeren we een service provider? Bijv. VC, certificaat, oid, FQDN etc.?

Geen revocation in de eerste pilot. Houd de levensduur van de VCs kort, geldigheid ruim houden tijdens voor tijdens de pilot.

Hosting van de JSON-LD context bij het GTK van VZVZ.

Nog geen delegation informatie tussen service provider en zorginstelling in de metadata van de AS.

DPOP buiten scope.

9.1.1 Authenticatie

Voor authenticatiemiddelen beperken we ons tot de UZI pas met zorgid. Dit betekent dat organisaties medewerkers met een een registratie in het UZI register nodig hebben voor het inschrijven van patienten en het mandateren van de organisatie voor de relevante bedrijfsrollen. In latere pilots zullen we gaan testen met de zogenoemde taakcodes. Deze maken het mogelijk voor niet-BIG geregistreerde medewerkers om toch een bedrijfsrol te krijgen en daarmee zonder mandaat toegang te krijgen voor transacties in de informatiestandaard.

9.1.2 Lokalisatie en brede bevraging

Sectie "brede bevraging" met audience binding is buiten scope van pilot 1. (10.8.4).

Omdat tijdens Pilot 1 er nog geen lokalisatiefunctie voor de raadplegende (Nuts) partijen beschikbaar is, wordt er gebruik gemaakt van de zogenaamde "brede bevraging" in het LSP. Hiervoor wordt er een access token aangevraagd voor het AS van het LSP in plaats van de bronhouder. Met dit access token wordt de FHIR functie $get-aorta-data gebruikt met als context parameter het gewenste dataset.

```
GET /rbgbc/fhir/R4/v1/$get-aorta-data?context=MEDGEG
```

Het GBC van het LSP zal op dat moment als verwerker van de raadpleger optreden en de volgende operaties uitvoeren:

1. Lokaliseren van relevante bronhouders van het gewenste dataset voor de patiënt
2. De adressen van de bronsystemen opvragen
3. De gegevens opvragen bij de bronsystemen
4. De gegevens consolideren volgens de regels van de informatiestandaard

9.2 Pilot 2

Pilot 1 + LSP partij die bij een Nuts partij iets op vraagt.

Beheer van de Credential-Repository in pilots:

Idealiter wordt dit allemaal door het LSP uitgevoerd, maar is het een goed idee om inschrijftokens en delegation tokens bij het LSP te leggen? Zo niet, kunnen we nu al vragen om zorginstellingen zelf een wallet te alten regelen in deze fase, dan wel aan LSP software leveranciers dit te implementeren?

Inloggen door mederwerkers zonder rol code via taakcodes.

10 Bijlage 1: Technische Specificaties

10.1 Inleiding

Doel van dit hoofdstuk: de technische keuzes vastleggen die specifiek zijn voor dit stelsel, zonder bestaande standaarden te herhalen. Dit hoofdstuk vormt de lijm tussen de normatieve referenties en beschrijft de stelsel-specifieke invullingen, profielen en extensies.

10.2 Normatieve referenties

Overzicht van alle gehanteerde standaarden met versie-pinning:

Standaard	Versie	Referentie
W3C Verifiable Credentials Data Model	1.1	https://www.w3.org/TR/2022/REC-vc-data-model-20220303/
W3C DID Core	1.0	https://www.w3.org/TR/did-core/
JSON Web Signature 2020	21-07-2022	https://w3c-ccg.github.io/lds-jws2020/
did:web Method Specification	(vast te pinnen)	https://w3c-ccg.github.io/did-method-web/
did:x509 Method Specification	(vast te pinnen)	ToIP / Microsoft
StatusList2021	(vast te pinnen)	W3C CCG
RFC 7515	-	JSON Web Signature (JWS)
RFC 7523	-	JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC 8414	-	OAuth 2.0 Authorization Server Metadata
RFC 9449	-	OAuth 2.0 Demonstrating Proof of Possession (DPoP)
IHE mCSD	(vast te pinnen)	Mobile Care Services Discovery
Nuts RFC023	-	X509Credential (extensie san:otherName)

10.3 Cryptografische parameters

Deze sectie specificeert de toegestane cryptografische algoritmen, sleuteltypes en transportbeveiliging per context. De keuzes zijn afgestemd op de beperkingen van de gebruikte hardware (met name de UZI-pas) en de gangbare praktijk binnen PKIoverheid.

10.3.1 did:web context

Credentials en presentaties die worden ondertekend met sleutelmateriaal behorend bij een did:web identifier MOETEN een van de volgende algoritmen gebruiken:

JWS alg	Algoritme	Curve / sleutellengte	Status
ES256	ECDSA	P-256 (secp256r1)	Aanbevolen

ES512	ECDSA	P-521 (secp521r1)	Toegestaan
PS256	RSASSA-PSS	RSA >= 2048 bits, SHA-256	NIET TOEPASSEN

- **ES256** is de aanbevolen keuze vanwege de balans tussen veiligheid, prestaties en brede ondersteuning in libraries en hardware.
- Het domein dat wordt gebruikt in een **did:web identifier** MOET een top-level domain (TLD) hebben met voldoende betrouwbaarheid en juridische afdwingbaarheid. Binnen dit stelsel is het gebruik van het **.nl verplicht**. Dit waarborgt dat domeinnamen vallen onder Nederlands recht en dat de SIDN als registerhouder voldoende garanties biedt ten aanzien van eigenaarschap en geschilbeslechting.
- **DID-documenten** voor did:web MOETEN worden gepubliceerd over **TLS 1.3 of hoger**. TLS 1.2 wordt nog voor beperkte tijd ondersteund. Het TLS-certificaat MOET afkomstig zijn van een vertrouwde certificaatautoriteit (zie sectie 8.6.1 voor de PKI-architectuur). Verdere eisen aan de structuur van het DID-document worden beschreven in sectie 10.4.

10.3.2 did:x509 context

Credentials die worden ondertekend met sleutelmateriaal behorend bij een did:x509 identifier zijn gebonden aan de mogelijkheden van het onderliggende X.509 certificaat en de bijbehorende hardware. De UZI-pas maakt gebruik van RSA-sleutels via de PKCS#11 interface.

De volgende algoritmen zijn toegestaan:

JWS alg	Algoritme	Sleutellengte	Status
PS256	RSASSA-PSS	RSA >= 2048 bits, SHA-256	Aanbevolen (komt Q4 - 2026)
RS256	RSASSA-PKCS1-v1_5	RSA >= 2048 bits, SHA-256	Toegestaan (legacy) (NU)

- **PS256** is de aanbevolen keuze omdat **RSASSA-PSS** een sterker beveiligingsprofiel biedt dan PKCS#1 v1.5.
- **RS256** is toegestaan voor compatibiliteit met bestaande UZI-certificaten en hardware die RSASSA-PSS niet ondersteunt.
- De **certificaatketen** MOET worden opgenomen in de **x5c header** parameter van het JWT conform RFC 7515 sectie 4.1.6. De certificaatketen MOET volledig zijn (van leaf tot root) en MOET gevalideerd worden volgens RFC 5280.
- De **x5t#S256 header** parameter MOET de SHA-256 thumbprint van het leaf-certificaat bevatten.

TLS1.3 toepassen

Signature Algorithms:
For verifying cryptographic tokens, we enforce the use of the following algorithms:

- **ES256** (Elliptic Curve P-256 with SHA-256) (NU)
- **ES512** (Elliptic Curve P-521 with SHA-512)
- ***PS256*** *(RSASSA-PSS with SHA-256) – Planned for future use (Q4-2026)*

Implementations must explicitly reject any other algorithms to ensure security and compliance with best practices.

For signing cryptographic tokens, one of the supported algorithms should be used.

Opmerking: naarmate de UZI-pas en PKIoverheid-certificaten evolueren naar ECDSA-ondersteuning, kunnen de toegestane algoritmen voor did:x509 worden uitgebreid. De specificatie voorziet in deze mogelijkheid doordat het sleuteltype wordt bepaald door het certificaat zelf.

10.3.3 DPoP

- **DPoP proofs** (RFC 9449) **MOETEN** worden ondertekend met **ES256 (ECDSA met P-256)**.
- De DPoP-sleutel is een **ephemeral (niet herbruikbaar)** sleutel die door de OAuth client wordt gegenereerd en is **niet gebonden aan een specifiek certificaat of DID**.
- Er wordt bewust slechts een enkel algoritme voorgeschreven om de **implementatielast te beperken.**

10.3.4 Overzicht per context

Context	Aanbevolen	Toegestaan	Niet toegestaan
did:web (VCs, VPs)	ES256	ES384, ES512, PS256	RS256, RS384, RS512
did:x509 (VCs)	PS256	RS256 (legacy)	Alle overige
DPoP proofs	ES256	-	Alle overige
TLS	TLS 1.3	TLS 1.2	TLS 1.1 en lager

Alle algoritmen die niet in de kolom "Aanbevolen" of "Toegestaan" staan, zijn NIET TOEGESTAAN. Implementaties MOETEN alle aanbevolen algoritmen ondersteunen en ZOUDEN alle toegestane algoritmen MOETEN ondersteunen. Verifiers MOETEN alle aanbevolen en toegestane algoritmen accepteren.

10.3.5 Sleutel levensduur

De levensduur van sleutelmateriaal verschilt per gebruiksdoel. Onderstaande richtlijnen zijn gebaseerd op NIST SP 800-57 Part 1 Rev 5 en afgestemd op de rollen in dit stelsel.

Rotatie en intrekking

Het onderscheid tussen sleutelrotatie en sleutelintrekking is essentieel. Bij rotatie wordt een sleutel vervangen door een nieuwe voor toekomstig gebruik, maar blijft de oude sleutel geldig voor verificatie van eerder gemaakte ondertekeningen. Bij intrekking wordt een sleutel ongeldig verklaard, ook voor eerder gemaakte ondertekeningen. In beide gevallen wordt de status van een sleutel bepaald door de publicatie van het sleutelmateriaal: een sleutel die als geldig is gepubliceerd (zie DID-documenten in de volgende sectie) wordt als geldig beschouwd; een sleutel die niet is gepubliceerd wordt als ongeldig beschouwd.

De wijze waarop publicatie wordt beheerd verschilt per DID-methode:

did:web: De organisatie beheert zelf het DID-document en kan sleutels direct toevoegen, behouden of verwijderen. Een geroteerde sleutel blijft gepubliceerd zolang er geldige credentials, ondertekend met deze sleutel, in omloop zijn. Bij compromittering wordt de sleutel onmiddellijk verwijderd.

did:x509: Het sleutelmateriaal is gebonden aan een X.509 certificaat dat wordt beheerd door een externe certificaatautoriteit. Na het verlopen van het certificaat worden CRL- en OCSP-diensten niet langer bijgewerkt, waardoor een gecompromitteerde maar verlopen sleutel niet meer te onderscheiden is van een legitieme. Om deze reden MOET de geldigheid van credentials die met did:x509 zijn ondertekend worden begrensd tot de geldigheidsduur van het onderliggende certificaat. Credential-level revocation via StatusList2021 (sectie 10.9) biedt hier een aanvullende verdedigingslinie: alle credentials die met een gecompromitteerde sleutel zijn uitgegeven MOETEN individueel worden ingetrokken.

Cryptoperiodes per sleuteltype

VC signing key *(assertionMethod)*: De cryptoperiode voor een private signing key is 1 tot 3 jaar (NIST SP 800-57, Tabel 1). Na afloop van de cryptoperiode MAG de sleutel niet meer worden gebruikt voor het uitgeven van nieuwe credentials.

VP signing key *(authentication)*: De cryptoperiode voor een private authentication key is 1 tot 2 jaar (NIST SP 800-57, Tabel 1). VP signing keys verwerken doorgaans een hoger transactievolume dan VC signing keys. NIST noemt het volume van transacties als factor bij het bepalen van de cryptoperiode; bij hoog gebruik kan een kortere cryptoperiode passend zijn.

DPoP key: De DPoP-sleutel is een ephemeral sleutel die per sessie of per transactie wordt gegenereerd. De levensduur is inherent beperkt tot de OAuth-sessie. Er is geen apart rotatie- of intrekkingsmechanisme nodig.

X.509 certificaten *(TLS, did:x509)*: De levensduur van X.509 certificaten wordt bepaald door de uitgevende certificaatautoriteit en valt buiten de scope van dit document. Deelnemers MOETEN certificaten tijdig vernieuwen en MOETEN de geldigheid van certificaten in de keten controleren bij verificatie.

10.4 DID-documenten

Een DID-document is het machine-leesbare document dat hoort bij een Decentralized Identifier (DID). Het bevat het publieke sleutelmateriaal van de eigenaar van de DID en beschrijft waarvoor elke sleutel mag worden gebruikt. Een verifier resolveert het DID-document om de publieke sleutel op te halen waarmee een handtekening kan worden geverifieerd. Hoe het DID-document wordt gepubliceerd en geresolveerd verschilt per DID-methode.

10.4.1 did:web

Resolutie

Het DID-document voor een did:web identifier wordt gepubliceerd op het domein van de deelnemer conform de did:web method specification. Het document MOET beschikbaar zijn op het relatieve pad `/.well-known/did.json` (voor domeinniveau DIDs) of op het overeenkomstige pad voor DIDs met een subpad.

Structuur

Het DID-document MOET minimaal de volgende velden bevatten:

- **id**: de did:web identifier van de deelnemer
- **verificationMethod** (optioneel): een lijst van publieke sleutels die eigendom zijn van deze DID, uitgedrukt als JWK (JSON Web Key, RFC 7517). Elke sleutel MOET een unieke id hebben (opgebouwd als `did:web:example.nl#key-1`) en een type van *JsonWebKey2020*
- **assertionMethod**: verwijzing(en) naar sleutel(s) die worden gebruikt voor het ondertekenen van Verifiable Credentials. Alleen partijen die de issuer-rol vervullen (zorginstellingen voor DelegationVCs, stelselhouder voor ServiceProviderCredentials) hoeven deze relationship op te nemen
- **authentication**: verwijzing(en) naar sleutel(s) die worden gebruikt voor het ondertekenen van Verifiable Presentations

Verwijzingen in assertionMethod en authentication MOGEN verwijzen naar verification methods in hetzelfde DID-document, maar MOGEN ook verwijzen naar verification methods in andere DID-documenten. De verificationMethod sectie MAG daarom leeg zijn indien alle sleutels elders zijn gedefinieerd.

De sleutels waarnaar assertionMethod en authentication verwijzen MOETEN verschillend zijn (AUTH-015). Dit beperkt de impact van compromittering: een sleutel waarmee presentaties worden ondertekend mag niet kunnen worden gebruikt om credentials uit te geven.

Sleutelrotatie

Bij sleutelrotatie (AUTH-017) wordt een nieuwe sleutel toegevoegd aan het DID-document. De oude sleutel hoeft niet direct te worden verwijderd: zolang er nog geldige credentials in omloop zijn die met de oude sleutel zijn ondertekend, en de sleutel niet is ingetrokken, MAG deze in het DID-document blijven staan. De oude sleutel MOET worden verwijderd zodra het laatste credential dat ermee is ondertekend is verlopen, of wanneer de sleutel wordt ingetrokken.

Verifiers MOETEN het DID-document ophalen bij verificatie en MOGEN het cachen conform de HTTP cache headers die het document meelevert.

10.4.2 did:x509

Een did:x509 identifier wordt **niet gepubliceerd als DID-document op een server**. Het DID-document wordt **lokaal afgeleid** (geresolved) op basis van de certificaatketen die wordt meegeleverd in de x5c header van het JWT (RFC 7515 sectie 4.1.6). Na resolutie is het certificaat als concept niet meer relevant: alle verdere validatie werkt uitsluitend op het DID-document en de daarin opgenomen keys en attributen.

Resolutie

De resolver voert de volgende stappen uit conform de did:x509 method specification:

1. Decodeer de certificaatketen uit de x5c header parameter
2. Valideer de certificaatketen conform RFC 5280 (handtekeningen, geldigheidsperiode, basic constraints)
3. Controleer dat de keten een geaccepteerde trust anchor bevat (sectie 10.4.2 trust anchors)
4. Controleer de revocation status van alle certificaten in de keten via CRL
5. Match de attributen in de DID-identifier tegen de velden in het certificaat
6. Construeer het DID-document

Let op: Een ingetrokken certificaat kan nog steeds een valide DID-document opleveren. Zie 10.4.3 over key-resolutie.

Structuur

Het resulterende DID-document bevat minimaal:

- `id`: de did:x509 identifier, inclusief alle attributen uit de DID policies
- `verificationMethod`: een of meerdere keys van type JsonWebKey2020, waarbij:
  - De publieke sleutel afkomstig is uit het leaf-certificaat
  - Het veld `expires` overeenkomt met de `notAfter` datum van het certificaat
  - Het veld `revoked` wordt gezet indien het certificaat op de CRL staat, met als waarde de revocation-datum

De DID-identifier zelf draagt de identificerende attributen (URA-nummer, organisatienaam, UZI-nummer, rolcode) via de DID policies. Na resolutie zijn deze attributen beschikbaar als onderdeel van de DID, niet als certificaatvelden.

Trust anchors

De ca-fingerprint in de did:x509 identifier bepaalt welke certificaatautoriteit wordt vertrouwd. De resolver MOET controleren dat de ca-fingerprint voorkomt in de lijst van geaccepteerde trust anchors voor het stelsel. De geaccepteerde trust anchors zijn intermediate CA-certificaten:

- PKIoverheid intermediate CA-certificaten die worden gebruikt voor de uitgifte van UZI-certificaten
- Toekomstige GIS-VN intermediate CA-certificaten

De exacte lijst van geaccepteerde ca-fingerprint waarden wordt beheerd als operationele configuratie en gepubliceerd door de stelselhouder. De set geaccepteerde trust anchors kan per credential type verschillen.

san:otherName extensie

De did:x509 method specification definieert een aantal DID policies waarmee attributen uit het certificaat worden opgenomen in de DID-identifier: subject, san (Subject Alternative Name) en eku (Extended Key Usage).

Nederlandse zorgcertificaten (UZI) bevatten identificerende attributen in het SubjectAlternativeName veld als otherName. Dit attribuut is niet standaard opgenomen in de did:x509 specificatie. Dit stelsel breidt de san DID policy uit met het otherName attribuut, conform Nuts RFC023 sectie 3.5.

Het otherName veld in UZI-certificaten is opgebouwd als `<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>`. De relevante velden hieruit worden als afzonderlijke attributen opgenomen in de DID-identifier. Voorbeeld:

```
did:x509:0:sha256:WE4P5dd8DnLHSkyHaIjhp4udlkF9LqoKwCvu9gl38jk::subject:O:Zieken
huis%20Voorbeeld::san:otherName:12345678
```

Hierbij is 12345678 het URA-nummer.

10.4.3 Key-resolutie

Naast DID-resolutie (het ophalen van het DID-document) kent dit stelsel het concept key-resolutie: het selecteren van de juiste publieke sleutel uit een DID-document op basis van een referentietijdstip.

Bij verificatie van een credential is het referentietijdstip de issuanceDate van het credential, niet het huidige tijdstip. Dit is essentieel omdat:

- Een sleutel die na uitgifte van het credential is ingetrokken of verlopen, ten tijde van uitgifte geldig was. De handtekening is dan nog steeds geldig.
- Bij sleutelrotatie (sectie 10.4.1) kunnen meerdere sleutels in een DID-document staan. De juiste sleutel wordt geselecteerd op basis van het tijdstip.

De key-resolutie werkt als volgt:

1. Selecteer de verification method die overeenkomt met de kid in de JWT header
2. Controleer dat de key geldig was op het referentietijdstip:
    a. Het referentietijdstip MOET voor de expires datum van de key liggen (indien aanwezig)
    b. De key MAG NIET als revoked gemarkeerd zijn met een revocation-datum die voor het referentietijdstip ligt
3. Controleer dat de key het juiste doel heeft (assertionMethod voor VCs, authentication voor VPs)

Dit mechanisme maakt het CRL-beleid voor inschrijftokens (sectie 10.6.5) en mandaattokens (sectie 10.6.4) uniform: als de key geldig was op het moment van uitgifte, is de handtekening geldig.

10.5 VC-encoding

Alle Verifiable Credentials in dit stelsel worden ge-encodeerd conform de W3C Verifiable Credentials Data Model 1.1, sectie 6.3.1 (JWT Encoding). Dit betekent dat een VC wordt verpakt als een signed JWT (JSON Web Token), waarbij de VC-velden worden gemapt op standaard JWT claims.

10.5.1 Mapping van VC-velden naar JWT claims

De volgende mapping wordt gehanteerd conform VC Data Model 1.1:

VC-veld	JWT claim	Toelichting
issuer	iss	DID van de issuer (did:web of did:x509)
credentialSubject.id	sub	DID van het subject (did:web)
issuanceDate	nbf	Uitgiftedatum als UNIX timestamp
expirationDate	exp	Verloopdatum als UNIX timestamp (indien van toepassing)
id	jti	Unieke identifier van het credential
Overige VC-velden	vc	Genest object met de volledige VC-structuur

Het vc claim bevat de volledige VC-structuur inclusief @context, type, credentialSubject en eventueel credentialStatus. De velden die al zijn gemapt naar JWT claims (iss, sub, nbf, exp) MOGEN worden weggelaten uit het vc object om duplicatie te voorkomen, maar MOETEN bij reconstructie van de VC weer worden aangevuld vanuit de JWT claims.

10.5.2 JWT header

De JWT header MOET de volgende velden bevatten:

Veld	Waarde	Toelichting
alg	Conform sectie 10.3	Signing-algoritme, afhankelijk van de DID-methode
typ	JWT	Token type
kid	Key ID	Voor did:web: verwijzing naar de verification method in het DID-document. Voor did:x509: de volledige DID met fragment
x5c	Certificaatketen	Alleen voor did:x509: de volledige certificaatketen in DER-formaat, base64-encoded. Alleen gebruikt bij **did:x509 issuers**
x5t#S256	SHA-256 thumbprint	Alleen voor did:x509: thumbprint van het leaf-certificaat.

10.5.3 Voorbeeld

Onderstaand voorbeeld toont een HealthcareProviderCredential als JWT. De header en payload zijn apart weergegeven; in de praktijk worden deze base64url-encoded en samengevoegd met een handtekening als header.payload.signature.

JWT header (did:x509 issuer):

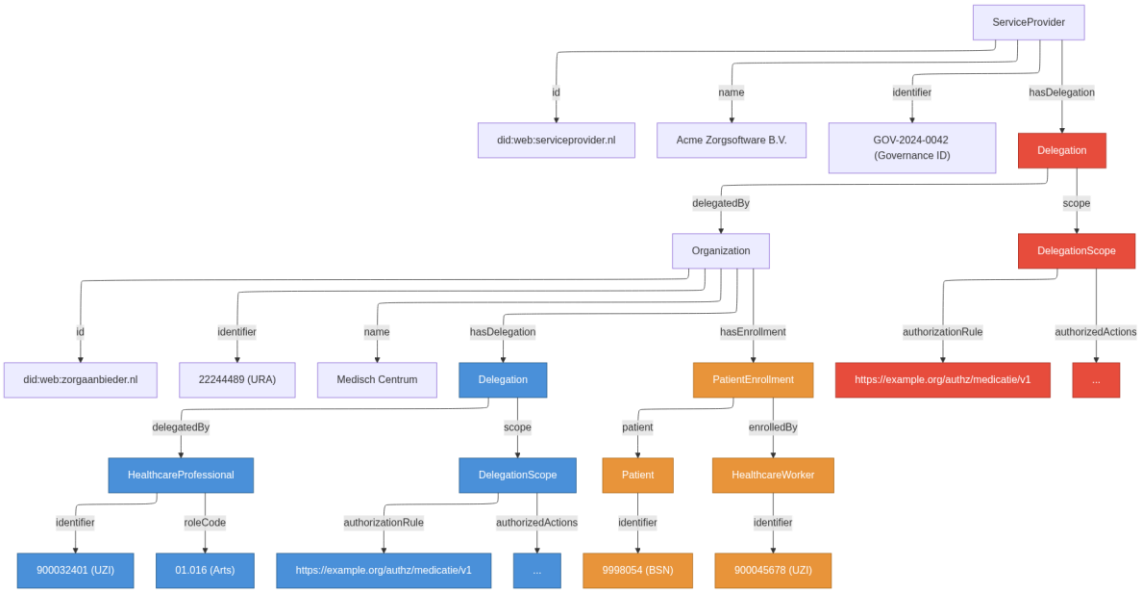
```
{
  "alg": "PS256",
  "typ": "JWT",
  "x5c": [
    "",
    "",
    ""
  ],
  "x5t#S256": "WE4P5dd8DnLHSkyHaIjhp4udlkF9LqoKwCvu9gl38jk",
  "kid":
"did:x509:0:sha256:WE4P5dd8DnLHSkyHaIjhp4udlkF9LqoKwCvu9gl38jk::subject
:O:Autoriteit::san:otherName:00000000#0"
}
```


JWT payload (met JSON-LD context) :


```
{
  "iss":
"did:x509:0:sha256:WE4P5dd8DnLHSkyHaIjhp4udlkF9LqoKwCvu9gl38jk::subject
:O:Autoriteit::san:otherName:00000000",
  "sub": "did:web:ziekenhuis-voorbeeld.nl",
  "nbf": 1733011200,
  "exp": 1764547200,
  "jti": "urn:uuid:3e671c46-7a3b-4c1e-9b2a-4f8e6d2c1a5b",
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://vzvz.nl/credentials/v1"
    ],
    "type": [
      "VerifiableCredential",
      "HealthcareProviderCredential"
    ],
    "credentialSubject": {
      "id": "did:web:ziekenhuis-voorbeeld.nl",
      "@type": "Organization",
      "identifier": {
        "system": " http://fhir.nl/fhir/NamingSystem/ura",
        "value": "12345678"
      },
      "name": "Ziekenhuis Voorbeeld"
    }
  }
}
```


In dit voorbeeld geeft een autoritatieve bron (geidentificeerd via did:x509 met een UZI-certificaat) een HealthcareProviderCredential uit aan een zorginstelling (geidentificeerd via did:web). De sub claim en credentialSubject.id verwijzen beide naar de did:web van de zorginstelling.

10.6 Credential-specificaties



Deze sectie specificeert per credential type de veldnamen, cardinaliteit en validatieregels. Alle credentials conformeren aan de encoding-regels uit sectie 10.5. Generieke validatieregels die voor meerdere credentials gelden staan in sectie 10.6.2. De credential-specifieke secties (10.6.3 t/m 10.6.7) beschrijven aanvullende regels per type.

10.6.1 JSON-LD context

Wat is JSON-LD?

JSON-LD (JSON for Linked Data) is een manier om gestructureerde gegevens uit te drukken in JSON, vergelijkbaar met hoe XML-namespaces en XML Schema structuur geven aan SAML assertions. De definitie wordt opgegeven in een @context veld en definieert het vocabulaire en zorgt ervoor dat alle partijen dezelfde betekenis toekennen aan de velden.

Stelsel-context

Alle credentials in dit stelsel maken gebruik van een gedeelde JSON-LD context die de ontologie definieert. De context specificeert de volgende namespaces:

- gis: http://gis-nl.example/ -- stelsel-specifieke termen
- schema: http://schema.org/ -- generieke termen (schema.org)

Context-definitie

```
{
  "@context": {
    "gis": "http://gis-nl.example/",
    "schema": "http://schema.org/",

    "HealthcareProvider": "gis:HealthcareProvider",
```

```
    "HealthcareProfessional": "gis:HealthcareProfessional",
    "HealthcareWorker": "gis:HealthcareWorker",
    "Patient": "gis:Patient",
    "ServiceProvider": "gis:ServiceProvider",

    "Delegation": "gis:Delegation",
    "DelegationScope": "gis:DelegationScope",
    "PatientEnrollment": "gis:PatientEnrollment",

    "Identifier": "schema:PropertyValue",
    "identifier": {
      "@id": "schema:identifier",
      "@container": "@set"
    },
    "system": "schema:propertyID",
    "value": "schema:value",
    "roleCode": {
      "@id": "gis:roleCode",
      "@type": "http://fhir.nl/fhir/NamingSystem/uzi-rolcode"
    },
    "name": "schema:name",

    "hasDelegation": "gis:hasDelegation",
    "delegatedBy": "gis:delegatedBy",
    "scope": "gis:scope",
    "authorizationRule": "gis:authorizationRule",
    "authorizedActions": "gis:authorizedActions",
    "hasEnrollment": "gis:hasEnrollment",
    "issuedTo": "gis:issuedTo",
    "patient": "gis:patient",
    "enrolledBy": "gis:enrolledBy",
    "services": "gis:services"
  }
}
```

Identifier-structuur

Identifiers worden gemodelleerd als geneste objecten met een system en value, naar het FHIR Identifier datatype. De onderliggende linked data representatie hergebruikt schema:PropertyValue uit schema.org, gealiast als Identifier voor leesbaarheid. De veldnamen system en value zijn aliases voor schema:propertyID en schema:value.

Alias	schema.org IRI	Beschrijving
Identifier	schema:PropertyValue	Type van het identifier-object
identifier	schema:identifier	Property die de identifier bevat (met @container: "@set" voor array-ondersteuning)
system	schema:propertyID	URI van het identifier-stelsel
value	schema:value	De waarde van de identifier

De volgende identifier-systemen worden gebruikt:

System URI	Beschrijving	Bron
http://fhir.nl/fhir/NamingSystem/ura	URA-nummer	UZI-register / LRZa
http://fhir.nl/fhir/NamingSystem/uzi-nr-pers	UZI-nummer persoon	UZI-certificaat (otherName)
http://fhir.nl/fhir/NamingSystem/bsn	Burgerservicenummer	GBA / SBV-Z

De roleCode is geen identifier maar een attribuut van de zorgverlener. Het wordt gedefinieerd als gis:roleCode met als datatype http://fhir.nl/fhir/NamingSystem/uzi-rolcode.

Entiteit-types

Type	IRI	Beschrijving
HealthcareProvider	gis:HealthcareProvider	Zorgaanbieder
HealthcareProfessional	gis:HealthcareProfessional	BIG-geregistreerde zorgverlener (zorgverlenerspas, pastype Z)
HealthcareWorker	gis:HealthcareWorker	Medewerker op naam (medewerkerspas op naam, pastype N). HealthcareProfessional is een subtype van HealthcareWorker
Patient	gis:Patient	Patient
ServiceProvider	gis:ServiceProvider	Dienstverlener (softwareleverancier)

Relatie-types

Type	IRI	Beschrijving
Delegation	gis:Delegation	Delegatie van bevoegdheid
DelegationScope	gis:DelegationScope	Scope waarbinnen de delegatie geldt
PatientEnrollment	gis:PatientEnrollment	Inschrijving van een patient bij een zorginstelling

Relatie- en attribuut-termen

Term	IRI	Beschrijving
hasDelegation	gis:hasDelegation	Verwijzing naar een delegatie
delegatedBy	gis:delegatedBy	De partij die de delegatie verleent
scope	gis:scope	Scope van de delegatie
authorizationRule	gis:authorizationRule	URI van de autorisatieregel
authorizedActions	gis:authorizedActions	Toegestane acties
hasEnrollment	gis:hasEnrollment	Verwijzing naar een inschrijving
issuedTo	gis:issuedTo	De organisatie ten behoeve waarvan het credential is uitgegeven
patient	gis:patient	De ingeschreven patient
enrolledBy	gis:enrolledBy	De uitvoerder van de inschrijving
services	gis:services	Lijst van diensten waarvoor een dienstverlener is toegelaten
name	schema:name	Naam van de entiteit

roleCode	gis:roleCode	UZI-rolcode (datatype fhirnl:uzi-rolcode)

Versiebeheer

Elke versie van een credential type wordt gepubliceerd als een specificatie door de stelselhouder. Deze specificatie omvat zowel de structuur (welke velden, welke types) als de governance-regels (maximale geldigheid, uitgifte-eisen, trust anchors, validatieregels).

Het versienummer is onderdeel van het credential type in het type veld en volgt een `.v<jaar>-<volgnummer>` notatie:

```
{
  "type": ["VerifiableCredential", "PatientEnrollmentCredential.v2026-1"]
}
```

Elke wijziging aan een credential type leidt tot een nieuw versienummer, ongeacht of het een structuurwijziging betreft (nieuw veld in credentialSubject) of een governance-wijziging (aangepaste geldigheidsregels, nieuwe trust anchors, aangescherpte uitgifte-eisen).

Een verifier die een onbekende versie ontvangt MOET het credential weigeren. De stelselhouder publiceert een lijst van actieve credential type versies.

Context-versie

De JSON-LD context definieert de vocabulaire (termen, types, IRIs). De context wordt gepubliceerd door de stelselhouder op een URI met een versienummer:

http://gis-nl.example/context/v1

Elk credential verwijst in het @context veld naar een specifieke versie van de context:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "http://gis-nl.example/context/v1"
  ]
}
```

De context-versie wijzigt alleen wanneer de vocabulaire verandert (nieuwe termen, gewijzigde IRIs, verwijderde definities). Governance-wijzigingen die de structuur niet raken (bv. aangepaste geldigheidsregels) vereisen geen nieuwe context-versie.

Voor het versiebeheer van de context gelden de volgende regels:

- **Toevoegen** van nieuwe termen, types of relaties is een minor wijziging en MOET backward compatible zijn. Bestaande credentials blijven geldig.
- **Wijzigen** van de IRI of het datatype van een bestaande term is een breaking change en vereist een nieuw versienummer.

- **Verwijderen** van een bestaande term is een breaking change en vereist een nieuw versienummer. Verifiers MOETEN credentials accepteren die verwijzen naar een oudere context-versie, mits die versie niet door de stelselhouder is ingetrokken. De stelselhouder publiceert een lijst van actieve context-versies.

De definitieve context-URI wordt gepubliceerd door de stelselhouder. Tot die tijd wordt http://gis-nl.example/ als placeholder gebruikt.

Structuurvalidatie

De JSON-LD context definieert de semantiek van de velden (wat betekenen ze), maar schrijft geen structuur voor (welke velden zijn verplicht, welke types zijn toegestaan, hoe ziet de nesting eruit). Een credential met semantisch ongeldige combinaties -- bijvoorbeeld een Patient met een hasDelegation -- wordt door een JSON-LD processor zonder fout verwerkt.

Voor structuurvalidatie biedt het W3C VC Data Model het credentialSchema mechanisme. Hiermee kan een issuer per credential type een JSON Schema publiceren dat de structuur van het credentialSubject valideert. Verifiers kunnen dit schema gebruiken om te controleren of een credential de verwachte velden bevat, de juiste nesting heeft en geen onverwachte structuren gebruikt.

Het JSON Schema wordt gevalideerd tegen de compacte JSON-vorm van het credential (niet de JSON-LD expanded form). Voor velden die door de JSON-LD context als @set zijn gedefinieerd (zoals identifier) accepteert het schema zowel een enkel object als een array via een oneOf constructie. Dit voorkomt dat implementaties die de waarde als enkel object of als array serialiseren onterecht worden afgewezen.

Een credential dat naar een JSON Schema verwijst bevat het volgende veld:

```
{
  "credentialSchema": {
    "id": "https://gis-nl.example/schemas/v1/healthcare-provider-
credential.json",
    "type": "JsonSchema"
  }
}
```

De JSON Schemas per credential type worden gepubliceerd door de stelselhouder. De schemas zijn opgenomen in Appendix A.

10.6.2 Generieke validatieregels

De volgende validatieregels gelden voor alle credentials in dit stelsel. Credential-specifieke secties verwijzen hiernaar en voegen alleen aanvullende regels toe.

Algemeen

1. Het credential MOET in JWT-encoding zijn conform sectie 10.5
2. Het type veld MOET VerifiableCredential bevatten plus het credential-specifieke type
3. De issuanceDate MOET in het verleden liggen
4. Indien expirationDate aanwezig is, MOET deze in de toekomst liggen
5. Het credentialSubject.id MOET een DID zijn dat door de verifier geresolveerd kan worden

DID- en key-resolutie

6. Het DID-document van de issuer MOET geresolveerd worden conform de toepasselijke DID-methode (sectie 10.4)
7. De signing key MOET geresolveerd worden via key-resolutie (sectie 10.4.3) met de issuanceDate van het credential als referentietijdstip
8. De key MOET geldig zijn geweest op het referentietijdstip: niet verlopen (expires) en niet ingetrokken (revoked) voor dat tijdstip
9. Identifier-waarden in het credentialSubject die afkomstig zijn uit de issuer DID (UZI-nummer, rolcode, URA-nummer) MOETEN overeenkomen met de corresponderende attributen in de issuer DID-identifier. De waarde wordt gelezen uit het identifier.value veld van het betreffende object, waarbij het identifier.system het identifier-stelsel aanduidt
10. De issuer DID MOET een geaccepteerde trust anchor bevatten. Welke trust anchors geaccepteerd zijn kan per credential type verschillen (zie de credential-specifieke secties)

Aanvullend bij did:web issuer

11. De signing key MOET voorkomen in de assertionMethod van het issuer DID-document
12. Het DID-document MOET gepubliceerd zijn over TLS 1.3 of hoger op een .nl domein (sectie 10.3.1)

10.6.3 HealthcareProviderCredential

Bewijst de identiteit van een zorgaanbieder. De zorgaanbieder geeft dit credential aan zichzelf uit op basis van de did:x509 identiteit die het URA-nummer bevat.

VC type: ["VerifiableCredential", "HealthcareProviderCredential"]

Issuer: did:x509 van de zorginstelling

Subject: did:web van de zorginstelling

Vereist pastype: S (servercertificaat)

Trust anchors: PKIoverheid intermediate CAs voor UZI-servercertificaten, of toekomstige GIS-VN intermediate CAs

Veld	IRI	Card.	Beschrijving/validatie
id	-	1	did:web van de zorginstelling
@type	-	1	HealthcareProvider (gis:HealthcareProvider)
identifier.@type	-	1	Identifier (schema:PropertyValue)
identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/ura
identifier.value	schema:value	1	URA-nummer, overeenkomend met het URA-nummer in de issuer DID
name	schema:name	1	Naam van de organisatie, overeenkomend met het subject:O attribuut in de issuer DID

Alle velden in de tabel zijn gescopet op credentialSubject.

Aanvullende validatieregels (naast sectie 10.6.2):

- Het pastype in de issuer DID MOET S zijn

- De name MOET overeenkomen met het subject:O attribuut in de issuer DID

10.6.3.1 HealthcareProfessionalDelegationCredential

Bewijst dat een zorgverlener bevoegdheid delegeert aan een zorginstelling. Dit is de VC-tegenhanger van het AORTA SAML mandaattoken. De zorgverlener ondertekent dit credential met de signing key van de UZI-zorgverlenerspas.

VC type: ["VerifiableCredential", "HealthcareProfessionalDelegationCredential"]

Issuer: did:x509 van de zorgverlener

Subject: did:web van de zorginstelling waarbinnen het mandaat geldig is

Vereist pastype: Z (zorgverlenerspas)

Trust anchors: PKIoverheid intermediate CAs voor UZI-zorgverlenerspassen, of toekomstige GIS-VN intermediate CAs

Veld	IRI	Card.	Beschrijving/validatie
id	-	1	did:web van de zorginstelling
@type	-	1	HealthcareProvider (gis:HealthcareProvider)
hasDelegation.@type	-	1	Delegation (gis:Delegation)
hasDelegation.issuedTo.@type	-		HealthcareProvider (gis:HealthcareProvider)
hasDelegation.issuedTo.identifier.@type	-		Identifier (schema:PropertyValue)
hasDelegation.issuedTo.identifier.system	schema:propertyID		http://fhir.nl/fhir/NamingSystem/ura
hasDelegation.issuedTo.identifier.value			URA-nummer van de zorginstelling ten behoeve waarvan het mandaat is uitgegeven
hasDelegation.delegatedBy.@type	-	1	HealthcareProfessional (gis:HealthcareProfessional)
hasDelegation.delegatedBy.identifier.@type	-	1	Identifier (schema:PropertyValue)
hasDelegation.delegatedBy.identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/uzi-nr-pers
hasDelegation.delegatedBy.identifier.value	schema:value	1	UZI-nummer van de zorgverlener, overeenkomend met de issuer DID
hasDelegation.delegatedBy.roleCode	gis:roleCode	1	UZI-rolcode van de zorgverlener, overeenkomend met de issuer DID
hasDelegation.scope.@type	-	1	DelegationScope (gis:DelegationScope)
hasDelegation.scope.authorizationRule	gis:authorizationRule	1	URI van de autorisatieregel waarbinnen het mandaat is uitgegeven

hasDelegation.scope.authorizedActions	gis:authorizedActions	1..*	Toegestane acties binnen de autorisatieregel

Alle velden in de tabel zijn gescopet op credentialSubject.

Het issuedTo veld bevat het URA-nummer van de zorginstelling ten behoeve waarvan het mandaat is uitgegeven. Dit is geen claim over de identiteit van het subject, maar een verklaring van de issuer over de organisatorische context van de uitgifte. De verifier MOET controleren dat het URA in issuedTo overeenkomt met het URA in het HealthcareProviderCredential dat in dezelfde Verifiable Presentation wordt gepresenteerd.

Aanvullende validatieregels (naast sectie 10.6.2):

- Het pastype in de issuer DID MOET Z zijn
- De expirationDate MOET voor of op de expires datum van de signing key liggen
- Het URA in `hasDelegation.issuedTo` MOET overeenkomen met het URA in het HealthcareProviderCredential in dezelfde VP

Scope: de waarden voor authorizationRule en authorizedActions worden bepaald door het toepasselijke afspraakstelsel. Welke waarden geldig zijn is nog niet vastgesteld (zie OV-012, OV-013).

10.6.4 PatientEnrollmentCredential

Bewijst dat een patiënt is ingeschreven bij een zorginstelling. Dit is de VC-tegenhanger van het AORTA SAML inschrijftoken. Het credential wordt ondertekend door een zorgverlener of medewerker op naam die de BSN-validatie heeft uitgevoerd.

VC type: ["VerifiableCredential", "PatientEnrollmentCredential"]

Issuer: did:x509 van de zorgverlener of medewerker die het credential ondertekent

Subject: did:web van de zorginstelling

Vereist pastype: Z (zorgverlenerspas) of N (medewerkerspas op naam)

Trust anchors: PKIoverheid intermediate CAs voor UZI-zorgverleners- en medewerkerspassen, of toekomstige GIS-VN intermediate CAs

Veld	IRI	Card.	Beschrijving
id	-	1	did:web van de zorginstelling
@type	-	1	HealthcareProvider (gis:HealthcareProvider)
hasEnrollment.@type	-	1	PatientEnrollment (gis:PatientEnrollment)
hasEnrollment.issuedTo.@type	-	1	HealthcareProvider (gis:HealthcareProvider)
hasEnrollment.issuedTo.identifier.@type	-	1	Identifier (schema:PropertyValue)
hasEnrollment.issuedTo.identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/ura

hasEnrollment.issuedTo.identifier.value	schema:value	1	URA-nummer van de zorginstelling ten behoeve waarvan de inschrijving is uitgegeven
hasEnrollment.patient.@type	-	1	Patient (gis:Patient)
hasEnrollment.patient.identifier.@type	-	1	Identifier (schema:PropertyValue)
hasEnrollment.patient.identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/bsn
hasEnrollment.patient.identifier.value	schema:value	1	BSN van de patient
hasEnrollment.enrolledBy.@type	-	1	HealthcareWorker (gis:HealthcareWorker)
hasEnrollment.enrolledBy.identifier.@type	-	1	Identifier (schema:PropertyValue)
hasEnrollment.enrolledBy.identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/uzi-nr-pers
hasEnrollment.enrolledBy.identifier.value	schema:value	1	UZI-nummer van de uitvoerder, overeenkomend met de issuer DID

Alle velden in de tabel zijn gescopet op credentialSubject.

Het `issuedTo` veld bevat het URA-nummer van de zorginstelling ten behoeve waarvan de inschrijving is uitgegeven. Dit is geen claim over de identiteit van het subject, maar een verklaring van de issuer over de organisatorische context van de uitgifte. De verifier MOET controleren dat het URA in `issuedTo` overeenkomt met het URA in het HealthcareProviderCredential dat in dezelfde Verifiable Presentation wordt gepresenteerd. Bij een URA-wijziging faalt deze controle, waardoor het credential effectief ongeldig wordt in de nieuwe context.

Het type HealthcareWorker wordt hier gebruikt ongeacht of de uitvoerder een zorgverlener (pastype Z) of medewerker op naam (pastype N) is. Aangezien HealthcareProfessional een subtype is van HealthcareWorker, past dit in beide gevallen. De rolcode is niet relevant voor de inschrijving en wordt daarom niet opgenomen.

Aanvullende validatieregels (naast sectie 10.6.2):

- Het pastype in de issuer DID MOET Z of N zijn
- De geldigheid van het credential is maximaal 18 maanden (conform het huidige AORTA beleid voor inschrijftokens)
- Het URA in `hasDelegation.issuedTo` MOET overeenkomen met het URA in het HealthcareProviderCredential in dezelfde VP

Het CRL-beleid voor inschrijftokens wordt afgehandeld door de generieke key-resolutie (sectie 10.4.3): de key wordt geresolveerd op basis van de issuanceDate van het credential. Als de key op dat moment geldig was en niet was ingetrokken, is de handtekening geldig, ook als de key later is ingetrokken.

10.6.5 ServiceProviderCredential

Bewijst dat een dienstverlener is toegelaten tot het stelsel. Dit credential wordt uitgegeven door de stelselhouder.

VC type: ["VerifiableCredential", "ServiceProviderCredential"]

Issuer: did:web van de stelselhouder (eventueel did:x509 indien de stelselhouder een X.509-gebaseerde identiteit gebruikt)

Subject: did:web van de dienstverlener

Veld	IRI	Card.	Beschrijving/validatie
id	-	1	did:web van de dienstverlener
@type	-	1	ServiceProvider (gis:ServiceProvider)
name	schema:name	1	Naam van de dienstverlener
services	gis:services	1..*	Lijst van diensten waarvoor de dienstverlener is toegelaten. Initieel wordt de waarde twiinGtK gebruikt om aan te geven dat de dienstverlener een Twiin-knooppunt opereert. Andere waarden worden gedefinieerd naarmate het stelsel groeit

Alle velden in de tabel zijn gescopet op credentialSubject.

Aanvullende validatieregels (naast sectie 10.6.2):

- De issuer MOET de stelselhouder zijn
- Indien de issuer een did:web is, MOET de signing key voorkomen in de assertionMethod van het issuer DID-document
- Het credential is geldig zolang de stelseltoelating van de dienstverlener geldig is

Opmerking: in de interimfase (zie sectie 8.3.2) kan de stelseltoelating worden vastgesteld op basis van PKIoverheid certificaten in combinatie met een allow-list in plaats van een expliciet credential.

10.6.6 ServiceProviderDelegationCredential

Bewijst dat een zorginstelling de dienstverlener machtigt om namens haar op te treden. De zorginstelling geeft dit credential uit aan de dienstverlener.

VC type: ["VerifiableCredential", "ServiceProviderDelegationCredential"]

Issuer: did:web van de zorginstelling

Subject: did:web van de dienstverlener

Veld	IRI	Card.	Beschrijving/validatie
id	-	1	did:web van de dienstverlener
@type	-	1	ServiceProvider (gis:ServiceProvider)
hasDelegation.@type	-	1	Delegation (gis:Delegation)
hasDelegation.delegatedBy.@type	-	1	HealthcareProvider (gis:HealthcareProvider)
hasDelegation.delegatedBy.identifier.@type	-	1	Identifier (schema:PropertyValue)
hasDelegation.delegatedBy.identifier.system	schema:propertyID	1	http://fhir.nl/fhir/NamingSystem/ura
hasDelegation.delegatedBy.identifier.value	schema:value	1	URA-nummer van de delegerende zorginstelling
hasDelegation.scope.@type	-	1	DelegationScope (gis:DelegationScope)
hasDelegation.scope.authorizationRule	gis:authorizationRule	1	URI van de autorisatieregel waarbinnen de delegatie geldt
hasDelegation.scope.authorizedActions	gis:authorizedActions	1..*	Toegestane acties, MOET een subset zijn van de services in het

			ServiceProviderCredential van de dienstverlener

Alle velden in de tabel zijn gescopet op credentialSubject.

Aanvullende validatieregels (naast sectie 10.6.2):

- De issuer MOET een did:web zijn van een zorginstelling met een geldig HealthcareProviderCredential
- De authorizedActions MOETEN een subset zijn van de services in het ServiceProviderCredential van de dienstverlener

Scope: de waarden voor authorizationRule en authorizedActions worden bepaald door het toepasselijke afspraakstelsel. Welke waarden geldig zijn is nog niet vastgesteld (zie OV-012, OV-013, OV-014)

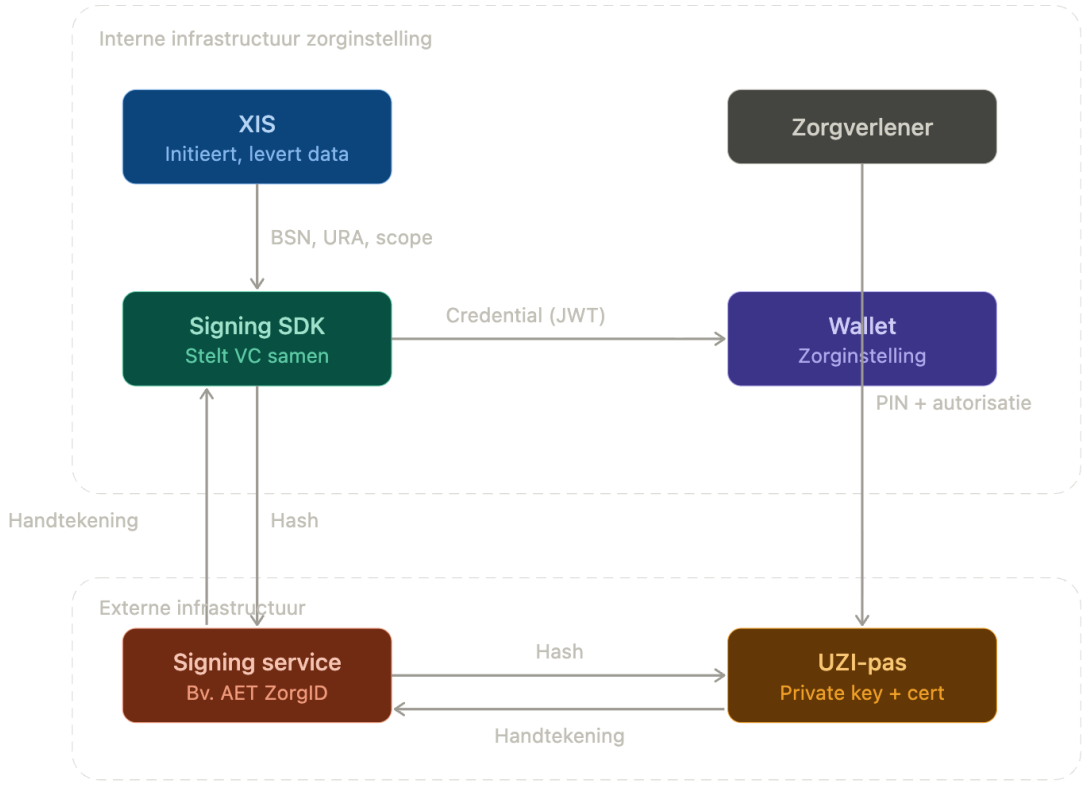
10.7 Credential-uitgifte (did:x509)

10.7.1 Overzicht

Deze sectie beschrijft het uitgifteproces voor credentials met een did:x509 issuer. Dit betreft credentials die worden ondertekend met de private key uit een UZI-certificaat: het HealthcareProviderCredential (servercertificaat), het HealthcareProfessionalDelegationCredential (zorgverlenerspas) en het PatientEnrollmentCredential (zorgverleners- of medewerkerspas).

Bij deze credentials is de issuer de zorgverlener, medewerker of zorginstelling zelf. De issuer-identiteit wordt vastgesteld op basis van het certificaat.

10.7.2 Architectuur



Het uitgifteproces maakt gebruik van een signing SDK die lokaal is geinstalleerd bij het XIS. De SDK neemt de cryptografische complexiteit uit handen: het samenstellen van het credential, het berekenen van de hash en het verkrijgen van de handtekening. Het XIS hoeft geen kennis te hebben van de onderliggende cryptografie.

De architectuur verschilt afhankelijk van het type certificaat:

Zorgverleners- of medewerkerspas (pastype Z of N): de private key staat op een smartcard en is niet direct toegankelijk voor de SDK. De SDK communiceert met een signing service die de hash doorstuurt naar de kaartlezer en de handtekening retourneert. De signing service ontvangt uitsluitend de hash, niet de credential-inhoud. De zorgverlener autoriseert de ondertekening door de PIN in te voeren. Een voorbeeld van een signing service is AET Europe met het ZorgID-platform.

Servercertificaat (pastype S): de private key is lokaal beschikbaar (via HSM of software-keystore). De SDK ondertekent het credential direct, zonder tussenkomst van een signing service en zonder eindgebruikerinteractie.

10.7.3 Uitgifteproces

Credentials met een zorgverleners- of medewerkerspas (pastype Z of N)

Dit betreft het PatientEnrollmentCredential en het HealthcareProfessionalDelegationCredential.

1. De zorgverlener plaatst de UZI-pas in de kaartlezer en voert de PIN in
2. De signing service zet een beveiligde sessie op met de pas en stelt de certificaatketen beschikbaar aan de SDK
3. Het XIS levert de aanvullende gegevens aan de SDK (zie sectie 10.7.4)
4. De SDK extraheert de identificerende attributen uit het certificaat (UZI-nummer, rolcode, pastype) en stelt het credential samen
5. De SDK berekent de hash van de JWT (header + payload) en stuurt deze via de signing service naar de UZI-pas
6. De UZI-pas ondertekent de hash met de private key en retourneert de handtekening via de signing service
7. De SDK assembleert de volledige JWT (header + payload + handtekening)
8. Het credential wordt opgeslagen in de wallet van de zorginstelling

HealthcareProviderCredential (pastype S)

Het HealthcareProviderCredential wordt ondertekend met een UZI-servercertificaat. Dit proces verloopt zonder eindgebruikerinteractie en zonder signing service:

1. Het XIS (of een geautomatiseerd proces) initieert de uitgifte via de SDK
2. Het XIS levert de aanvullende gegevens aan de SDK (zie sectie 10.7.4)
3. De SDK verkrijgt de certificaatketen van het servercertificaat en stelt het credential samen
4. De SDK ondertekent de JWT direct met de lokaal beschikbare private key
5. Het credential wordt opgeslagen in de wallet van de zorginstelling

10.7.4 Aanvullende gegevens

Het XIS levert de gegevens aan die niet uit het certificaat afkomstig zijn. De SDK combineert deze met de certificaat-attributen om het volledige credential samen te stellen.

Credential	Uit certificaat	Aangeleverd door XIS
HealthcareProviderCredential	URA, organisatienaam	--
HealthcareProfessionalDelegationCredential	UZI-nummer, rolcode	URA zorginstelling, scope (authorizationRule, authorizedActions)
PatientEnrollmentCredential	UZI-nummer, pastype	BSN van de patient

Het XIS is verantwoordelijk voor de juistheid van de aangeleverde gegevens. Bij het PatientEnrollmentCredential heeft de zorgverlener of medewerker het BSN gevalideerd conform de geldende procedures (SBV-Z/GBA-verificatie). Het stelsel vertrouwt deze validatie.

De aanvullende gegevens worden aangeleverd als een JSON-LD fragment van het credentialSubject met de stelsel-context, bevattend uitsluitend de waarden die niet uit het certificaat afkomstig zijn:

```
{
  "@context": "http://gis-nl.example/context/v1",
  "@type": "HealthcareProvider",
  "hasEnrollment": {
    "patient": {
      "@type": "Patient",
      "identifier": {
        "@type": "Identifier",
```

```
        "system": "http://fhir.nl/fhir/NamingSystem/bsn",
        "value": "999911234"
      }
    }
  }
}
```

De SDK valideert dat de aangeleverde gegevens passen bij het gevraagde credential type.

10.7.5 Beveiliging

Bij credentials met een zorgverleners- of medewerkerspas ontvangt de signing service uitsluitend een hash van het credential, niet de inhoud. Dit waarborgt dat gevoelige gegevens (met name BSN) niet buiten het XIS komen tijdens het ondertekeningsproces.

De communicatie tussen de SDK en de signing service MOET over een beveiligd kanaal verlopen (TLS). De sessie tussen de signing service en de UZI-pas wordt beveiligd door het PKCS#11 protocol van de smartcard.

De SDK MOET controleren dat het (pas)type in het certificaat past bij het gevraagde credential type: Z voor een HealthcareProfessionalDelegationCredential, Z of N voor een PatientEnrollmentCredential en S voor een HealthcareProviderCredential.

10.7.6 Integratie met het XIS

De signing SDK kan op twee manieren worden geïntegreerd met het XIS:

Als library: de SDK wordt als softwarebibliotheek opgenomen in het XIS. De interface is niet gestandaardiseerd en wordt bepaald door de SDK-leverancier. Voor dit ontwerp is deze route out-of-scope.

Als service: de SDK wordt als zelfstandige service gehost in de interne infrastructuur van de zorginstelling, bijvoorbeeld als container. In dit geval biedt de service een interface aan op basis van OpenID4VCI, wat een gestandaardiseerd koppelvlak oplevert tussen het XIS en de signing service. Tijdens de pilots maken we gebruik van ZorgID aangeboden door AET.

OpenID4VCI profiel voor de service-variant

Wanneer de SDK als service draait, worden de drie koppelvlakken van OpenID4VCI als volgt ingevuld (zorg id wordt hier als voorbeeld implementatie gebruikt):

1. Authorization endpoint (smartcard-sessie): het XIS redirect de gebruiker naar een pagina van de ZORG-ID-service. Deze pagina initieert de smartcard-sessie via een `zorgid://` link, waarmee de ZorgID desktop client wordt geopend. De zorgverlener plaatst de pas en voert de PIN in. Na succesvolle authenticatie redirect de ZORG-ID-service terug naar het XIS met een authorization code.

Bij credentials met een servercertificaat (pastype S) is er geen gebruikersinteractie en wordt de authorization stap overgeslagen of geautomatiseerd afgehandeld.

2. Token endpoint (sessie-binding): het XIS wisselt de authorization code in voor een access token bij de ZORG-ID-service. Het access token vertegenwoordigt de actieve sessie met het certificaat en bindt de daaropvolgende credential requests aan de geauthenticeerde zorgverlener.

3. Credential endpoint (credential-aanvraag): het XIS stuurt een credential request naar de lokale SDK-service met:

- Het **access token** als sessiebinding
- De **credential_configuration_id** die het credential type aanduidt
- Een **proof** JWT ondertekend door de zorginstelling (did:web), met in de kid header een DID URL die verwijst naar de authentication key van de zorginstelling. De SDK leidt hieruit het subject-DID af voor het credential
- De **credential_subject_data** als JSON-LD fragment met de aanvullende gegevens (sectie 10.7.4)

De SDK-service valideert het request, stelt het credential samen op basis van de certificaat-attributen en de aangeleverde gegevens, verkrijgt de handtekening (lokaal bij servercertificaat, via de signing service bij een pas) en retourneert het credential.

Het subject-DID van het credential (de did:web van de zorginstelling) wordt doorgegeven via de kid header in de proof JWT. De OpenID4VCI specificatie definieert dat de kid een DID URL is die verwijst naar de key waaraan het credential wordt gebonden. De SDK resolveert deze DID en gebruikt het als credentialSubject.id.

Voorbeeld credential request voor een PatientEnrollmentCredential:

```
POST /credential HTTP/1.1
Host: sdk-service.intern.zorginstelling.nl
Authorization: Bearer <access_token>
Content-Type: application/json

{
  "credential_configuration_id": "PatientEnrollmentCredential",
  "proof": {
    "proof_type": "jwt",
    "jwt":
"eyJ0eXAiOiJvcGVuaWQ0dmNpLXByb29mK2p3dCIsImFsZyI6IkVTMjU2Iiwia2lkIjoiZG
lkOndlYjpodWlzYXJ0cy1kZWxpbmRlbi5ubCNhdXRoLWtleS0xIn0.eyJhdWQiOiJodHRwc
zovL3Nkay1zZXJ2aWNlLmludGVybi56b3JnaW5zdGVsbGluZy5ubCIsImlhdCI6MTc0MDAw
MDAwMCwibm9uY2UiOiJhYmMxMjMifQ.kort-handtekening"
  },
  "credential_subject_data": {
    "@context": "http://gis-nl.example/context/v1",
    "@type": "HealthcareProvider",
    "hasEnrollment": {
      "patient": {
        "@type": "Patient",
        "identifier": {
          "@type": "Identifier",
          "system": "http://fhir.nl/fhir/NamingSystem/bsn",
          "value": "999911234"
        }
      }
    }
  }
}
```

De proof JWT bevat in de decoded header kid: "did:web:huisarts-delinden.nl#auth-key-1", waarmee de SDK het subject-DID afleidt. De JWT is ondertekend met de corresponderende private key van de zorginstelling, wat key possession bewijst.

Dit model biedt een gestandaardiseerd koppelvlak waardoor het XIS onafhankelijk is van de specifieke SDK-leverancier.

10.7.7 Credential-uitgifte voor did:web

Credentials met een did:web issuer (ServiceProviderCredential, ServiceProviderDelegationCredential) worden niet via het hierboven beschreven proces uitgegeven. Deze credentials worden samengesteld en ondertekend door de issuer zelf (de stelselhouder respectievelijk de zorginstelling) met sleutelmateriaal dat direct beschikbaar is. Hiervoor is geen signing SDK of signing service nodig.

10.8 Verifiable Presentations

10.8.1 Overzicht

Een Verifiable Presentation (VP) is een door de holder ondertekend pakket van een of meer Verifiable Credentials. De VP bindt de credentials aan een specifieke context (audience) en bewijst dat de holder beschikt over het sleutelmateriaal dat bij de credentials hoort.

Bij een token request worden twee VPs aangeboden, gegroepeerd op subject (zie sectie 8.4.1):

VP 1: Zorginstelling: bevat de credentials die over de zorginstelling gaan. Ondertekend met sleutelmateriaal van de zorginstelling (did:web).

Credential	Altijd aanwezig
HealthcareProviderCredential	Ja
HealthcareProfessionalDelegationCredential	Afhankelijk van de toepassing
PatientEnrollmentCredential	Afhankelijk van de toepassing

VP 2: Dienstverlener: bevat de credentials die over de dienstverlener gaan. Ondertekend met sleutelmateriaal van de dienstverlener (did:web).

Credential	Altijd aanwezig
ServiceProviderCredential	Ja
ServiceProviderDelegationCredential	Ja

Deze groepering volgt het standaard VP-model: de issuer van de VP is het subject van de credentials in die VP. Dit voorkomt dat een partij credentials presenteert die over een andere partij gaan zonder dat die andere partij daar cryptografisch aan meewerkt.

10.8.2 Structuur

Een VP in dit stelsel MOET in JWT-encoding zijn. De JWT bevat de volgende claims:

- `iss`: de DID van de holder (ondertekende partij)
- `aud`: de audience waarvoor de VP bestemd is (zie sectie 10.7.3)

- `iat`: tijdstip van uitgifte
- `nbf`: tijdstip vanaf wanneer de VP geldig is
- `exp`: tijdstip waarop de VP verloopt. De maximale geldigheid van een VP is 10 seconden na uitgifte (`exp` MOET kleiner of gelijk zijn aan `iat` + 10 seconden)
- `vp`: het VP-object met daarin:
    - `@context: ["https://www.w3.org/2018/credentials/v1"]`
    - `type: ["VerifiablePresentation"]`
    - verifiableCredential: een lijst van credentials in JWT-encoding

De VP JWT MOET ondertekend zijn met een sleutel uit de authentication verification relationship van het DID-document van de holder (sectie 10.4.1). De gebruikte sleutel MOET verschillen van de sleutel in assertionMethod (AUTH-015).

10.8.3 Audience binding

De VP wordt gebonden aan de ontvangende partij via het aud claim in de JWT. De waarde van aud MOET de issuer identifier van de authorization server zijn waarnaar het token request wordt gestuurd (sectie 8.5.3).

Voorbeeld: indien het token request wordt gestuurd naar de AS met identifier `https://as.dienstverlener.nl/tenant/12345678`, dan MOET `aud` in beide VPs deze waarde bevatten.

De audience binding voorkomt dat een onderschepte VP kan worden hergebruikt bij een andere authorization server.

10.8.4 Brede bevragingen en audience binding

Probleem

In het LSP-model doet een raadpleger een enkel verzoek aan het LSP, waarna het LSP lokaliseert, alle relevante bronhouders bevraagt, en de resultaten samengevoegd terugstuurt. De raadpleger weet niet welke bronhouders worden bevraagd -- dit is bewust transparant (HAR-010).

Dit conflicteert met de audience binding uit sectie 10.7.3: als de audience in de VP gebonden is aan de AS van een specifieke bronhouder, moet de raadpleger vooraf weten welke bronhouders er zijn en voor elke bronhouder een afzonderlijke VP maken. Dat doorbreekt de transparantie van het LSP-model.

Oplossing

Er zijn twee oplossingen die naast elkaar kunnen bestaan. De keuze hangt af van de fase en de mate van wallet-adoptie bij de achterliggende zorginstellingen.

Optie 1: het LSP beheert de wallet

Het LSP beheert als dienstverlener de volledige wallet voor de bij het LSP aangesloten zorginstellingen. Het LSP heeft directe toegang tot de credentials en het sleutelmateriaal van de zorginstelling, en kan zelfstandig VPs samenstellen met de juiste audience voor elke bronhouder.

Deze optie is met name interessant in de eerste fase van het stelsel, omdat er geen afhankelijkheid is van de achterliggende leveranciers voor het beschikbaar hebben van een wallet-implementatie.

Optie 2: herverpakking via gedeelde keys

De zorginstelling beheert haar eigen wallet en maakt een VP met als audience de dienstverlener (het LSP). Het LSP ontvangt de VP, valideert deze, en pakt de credentials uit. Voor elke bronhouder die bevraagd moet worden, verpakt het LSP de credentials opnieuw in een nieuwe VP met de juiste audience (de AS van de betreffende bronhouder).

Dit is mogelijk doordat het DID-document van de zorginstelling naast de eigen authentication key ook een key bevat die wordt beheerd door het LSP. De nieuwe VP wordt ondertekend met deze key. De bronhouder valideert de VP en ziet dat de signing key voorkomt in de authentication relationship van het DID-document van de zorginstelling. De VP is geldig, ondanks dat deze niet door de zorginstelling zelf is ondertekend.

De credentials zelf blijven ongewijzigd; alleen de VP-verpakking verandert.

Beide opties zijn in lijn met AUTH-014: de holder bepaalt welke credentials worden gepresenteerd en aan wie. Bij optie 1 is deze bevoegdheid operationeel gedelegeerd aan het LSP via het wallet-beheer. Bij optie 2 geeft de zorginstelling expliciet toestemming door de key van het LSP op te nemen in haar DID-document.

Relatie met de wallet-architectuur

Deze inrichting past bij de wallet-architectuur uit sectie 8.4.2: de zorginstelling is juridisch eigenaar van de wallet, maar het operationeel beheer kan bij de dienstverlener liggen. De key in het DID-document is de technische uitdrukking van deze delegatie.

10.8.5 Validatie

De authorization server valideert de ontvangen VPs in drie fasen: eerst wordt elke VP individueel gevalideerd, daarna worden de VP-specifieke eisen gecontroleerd, en tot slot wordt de relatie tussen de VPs geverifieerd.

Fase 1: validatie per VP

De volgende stappen worden uitgevoerd voor elke ontvangen VP:

1. Lees de iss claim uit de JWT payload. Dit is de DID van de holder
2. Lees de kid uit de JWT header. Dit identificeert de specifieke signing key
3. Resolveer het DID-document van de iss DID
4. Controleer dat de kid voorkomt in de authentication relationship van het DID-document van de iss. De kid MAG verwijzen naar een verification method in hetzelfde DID-document of naar een verification method in een ander DID-document (sectie 10.7.4 optie 2)
5. Resolveer de publieke sleutel: indien de kid verwijst naar een lokale verification method, gebruik die sleutel. Indien de kid verwijst naar een externe verification method, resolveer het DID-document waarnaar de kid verwijst en haal daar de publieke sleutel op
6. Verifieer de JWT-handtekening met de geresolveerde publieke sleutel
7. Controleer dat het aud claim overeenkomt met de eigen issuer identifier van de AS
8. Controleer dat nbf in het verleden ligt en exp in de toekomst ligt
9. Controleer dat exp kleiner of gelijk is aan iat + 10 seconden
10. Controleer dat de iss claim overeenkomt met het credentialSubject.id van de credentials in de VP
11. Valideer elk credential in de VP conform de generieke (sectie 10.6.2) en credential-specifieke validatieregels

Fase 2: validatie per VP-type

1. Controleer dat VP 1 (zorginstelling) ten minste een HealthcareProviderCredential bevat
2. Controleer dat VP 2 (dienstverlener) ten minste een ServiceProviderCredential en een ServiceProviderDelegationCredential bevat

Fase 3: validatie van de relatie tussen VPs

14. Controleer dat de issuer van de ServiceProviderDelegationCredential in VP 2 overeenkomt met de iss van VP 1

10.9 Revocation

10.9.1 Overzicht

Dit stelsel kent twee mechanismen voor het intrekken van credentials:

- **CRL (Certificate Revocation List)**: voor credentials met een did:x509 issuer. De revocation status wordt bepaald tijdens DID-resolutie en is beschikbaar als revoked veld op de key in het DID-document (sectie 10.4.2). Dit mechanisme wordt beheerd door de certificaatautoriteit (UZI-register) en valt buiten de scope van dit hoofdstuk.
- **StatusList2021**: voor credentials met een did:web issuer en voor langlopende credentials waar intrekking los van de certificaat-levenscyclus nodig is.

10.9.2 Toepasselijkheid

Credential	Revocation-mechanisme	Toelichting
HealthcareProviderCredential	CRL (via key-resolutie)	Intrekking volgt de levenscyclus van het servercertificaat
HealthcareProfessionalDelegationCredential	StatusList2021	Intrekking nodig wanneer de zorgverlener de organisatie verlaat, onafhankelijk van de certificaatgeldigheid
PatientEnrollmentCredential	CRL (via key-resolutie)	Geldigheid beperkt tot 18 maanden; intrekking bij vertrek patient is operationeel proces
ServiceProviderCredential	StatusList2021	Stelselhouder kan toelating intrekken
ServiceProviderDelegationCredential	StatusList2021	Zorginstelling kan delegatie intrekken

10.9.3 StatusList2021

Werking

StatusList2021 is een mechanisme waarbij de issuer van een credential een bitstring publiceert als Verifiable Credential. Elke bit in de string correspondeert met een credential. Een bit met waarde 0 betekent "niet ingetrokken", een bit met waarde 1 betekent "ingetrokken". De bitstring wordt gecomprimeerd met GZIP om de omvang te beperken.

Het credential dat intrekbaar is bevat een verwijzing naar de status list:

- `credentialStatus.type`: StatusList2021Entry
- `credentialStatus.statusPurpose`: revocation
- `credentialStatus.statusListIndex`: de positie van de bit in de lijst
- `credentialStatus.statusListCredential`: de URL waar de status list credential te vinden is

De verifier haalt de status list credential op, decomprimeert de bitstring en controleert de bit op de opgegeven index.

Status list credential

De status list zelf wordt gepubliceerd als een Verifiable Credential van type StatusList2021Credential. Dit credential:

- MOET in JWT-encoding zijn
- MOET ondertekend zijn door dezelfde issuer als het credential waarnaar het verwijst
- MOET beschikbaar zijn op een HTTPS endpoint
- MOET het veld credentialSubject.type bevatten met waarde StatusList2021
- MOET het veld credentialSubject.statusPurpose bevatten met waarde revocation
- MOET het veld credentialSubject.encodedList bevatten: de GZIP-gecomprimeerde, base64-gecodeerde bitstring

Caching

Verifiers MOGEN de status list credential cachen. De issuer MOET HTTP cache headers meegeven die aangeven hoe lang de status list geldig is. De maximale cache-duur is afhankelijk van het risicoprofiel:

- ServiceProviderCredential: maximaal 24 uur
- ServiceProviderDelegationCredential: maximaal 24 uur
- HealthcareProfessionalDelegationCredential: maximaal 24 uur

Kortere cache-duren zijn toegestaan. De issuer bepaalt de juiste balans tussen actualiteit en belasting.

10.9.4 Publicatie en hosting

De issuer van een credential is verantwoordelijk voor het publiceren van de bijbehorende status list. De status list URL wordt opgenomen in het credential zelf (via credentialStatus.statusListCredential) en MOET een HTTPS endpoint zijn.

Voor credentials met een did:web issuer (ServiceProviderCredential, ServiceProviderDelegationCredential) is de hosting eenvoudig: de issuer publiceert de status list op een eigen endpoint.

Hosting bij did:x509 issuers

Bij credentials met een did:x509 issuer beschikt de issuer doorgaans niet over een eigen server om een status list te hosten. De partij die de tooling levert voor het aanmaken van het credential (momenteel EAT Europe) host de status list namens de issuer.

In de huidige inrichting kan alleen de issuer zelf -- de houder van de UZI-pas -- een credential intrekken. De intrekking wordt geauthenticeerd met dezelfde pas waarmee het credential is uitgegeven.

Dit model kent een aantal beperkingen die latere uitwerking vragen:

- De zorginstelling kan een credential niet intrekken wanneer een medewerker de organisatie verlaat, ook niet in een conflictsituatie
- Indien de UZI-pas is verlopen, ingetrokken of verloren, kan de issuer geen intrekking meer uitvoeren terwijl er nog geldige credentials in omloop kunnen zijn
- Het is onduidelijk wie de intrekkingsbevoegdheid krijgt wanneer de oorspronkelijke issuer niet meer beschikbaar is

Deze vraagstukken raken de governance van het stelsel en worden in een volgende fase uitgewerkt.

10.9.5 Verificatie

Bij verificatie van een credential dat een credentialStatus veld bevat, MOET de verifier de volgende stappen uitvoeren:

1. Haal de status list credential op van de URL in credentialStatus.statusListCredential, of gebruik een gecachte versie indien de cache nog geldig is
2. Verifieer de handtekening van de status list credential
3. Controleer dat de issuer van de status list credential overeenkomt met de issuer van het te verifieren credential
4. Decomprimeer de bitstring uit credentialSubject.encodedList
5. Lees de bit op de positie aangegeven door credentialStatus.statusListIndex
6. Indien de bit waarde 1 heeft: het credential is ingetrokken en MOET worden geweigerd

Indien de status list credential niet opgehaald kan worden (netwerk fout, endpoint niet beschikbaar), MOET de verifier het credential weigeren. Dit voorkomt dat een aanvaller door het onbereikbaar maken van de status list ingetrokken credentials kan hergebruiken.

10.10 OAuth-profiel

10.10.1 Overzicht

Het OAuth-profiel in dit stelsel is gebaseerd op RFC 7523 (JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants) in combinatie met Verifiable Presentations. Het profiel onderscheidt twee rollen in het token request:

- **Client**: de dienstverlener, die zich authenticert via een client assertion (VP 2)
- **Subject**: de zorginstelling, namens wie het verzoek wordt gedaan, die zich authenticeert via een JWT als authorization grant (VP 1)

Dit onderscheid is essentieel omdat de partij die het technische verzoek doet (de dienstverlener) niet dezelfde is als de partij die de bevoegdheid heeft (de zorginstelling). Zie sectie 8.5.1.

De flow is back-channel: er is geen user-agent redirect (OAUTH-004). Het token request gaat rechtstreeks van de client naar de authorization server van de bronhouder.

10.10.2 Scope-model

Het token request bevat een scope die uit twee lagen bestaat:

Use-case scope

De use-case scope selecteert welk autorisatiebeleid van toepassing is en welke credentials de authorization server verwacht. Voorbeelden van use-case scopes zijn "urn:mo:voorschrijven:v1", "urn:eo:sender". Belangrijk is om te zorgen dat deze scopes uniek zijn in het stelsel. Een manier om dat te bereiken is een namespace van programma of stelsel toe te passen met daar achter een namespace. Versioning kan gedaan worden door een vx toe te voegen.

De use-case scope bepaalt:

- Welke credentials verplicht zijn in de presentatie (bv. wel of geen PatientEnrollmentCredential)
- Welk autorisatiebeleid de AS toepast bij het beoordelen van het verzoek
- Welke resource scopes beschikbaar zijn binnen deze use case
- Welke request-time controles er nog moeten worden verricht.

De use-case scope wordt uitgedrukt als een identifier. De waarden hiervan zijn nog niet definitief vastgesteld en hangen samen met de scope-architectuur die wordt beschreven in sectie 8.5.5 en de onderzoeksvragen OV-012, OV-013 en OV-014.

Resource scope

De resource scope specificeert welke concrete resources worden opgevraagd. Voor FHIR-gebaseerde uitwisselingen wordt het SMART-on-FHIR scope-formaat gebruikt (OAUTH-009), bijvoorbeeld patient/MedicationRequest.s.

De resource scope wordt gevalideerd door de AS tegen de bevoegdheden in de gepresenteerde credentials (rolcode, authorizedActions) en tegen de use-case scope.

Samenhang

Bij een token request worden beide scope-niveaus gecombineerd. Voorbeeld:

```
scope=urn:mo:voorschrijven:v1
patient/MedicationRequest.s?category=http://snomed.info/sct|16076005
```

Hierbij is `urn:mo:voorschrijven:v1` de use-case scope die het autorisatiebeleid selecteert, en de overige waarden zijn SMART-on-FHIR resource scopes.

10.10.3 Token endpoint

Het token endpoint van de AS kan zorgorganisatie onafhankelijk zijn. De relatie van het request met de zorginstelling is af te leiden uit de audience van de assertions. Deze moet gelijk zijn aan de zorginstelling specifieke AS identifier.

https://as.dienstverlener.nl/token

Het token endpoint wordt gepubliceerd in de AS metadata (sectie 10.9.4).

10.10.4 AS metadata

De authorization server publiceert metadata conform RFC 8414. De metadata is beschikbaar op het .well-known pad dat wordt afgeleid van de issuer identifier:

Issuer: https://as.dienstverlener.nl/tenant/12345678
Metadata: https://as.dienstverlener.nl/.well-known/oauth-authorization-server/tenant/12345678

Het metadata-document MOET minimaal de volgende velden bevatten:

- issuer: de issuer identifier van de AS

- token_endpoint: de URL van het token endpoint
- grant_types_supported: MOET urn:ietf:params:oauth:grant-type:jwt-bearer bevatten (RFC 7523)
- token_endpoint_auth_methods_supported: MOET private_key_jwt bevatten
- token_endpoint_auth_signing_alg_values_supported: MOET de algoritmen uit sectie 10.3.1 bevatten
- dpop_signing_alg_values_supported: MOET ES256 bevatten (sectie 10.3.3) (deze is buiten scope voor PoC/Pilot 1)

10.10.5 Verificatie van de delegatierelatie

Probleem

In dit stelsel wordt (m)TLS uitsluitend gebruikt voor transportbeveiliging op netwerklaag, niet voor het authenticeren van partijen. Een client die een token request stuurt naar een AS heeft daardoor geen TLS-gebaseerde garantie dat de AS daadwerkelijk opereert namens de zorginstelling waarmee het wil communiceren. Het adresboek (Care Services Directory) wordt hiervoor niet als een voldoende vertrouwde bron beschouwd.

De client heeft een cryptografisch bewijs nodig dat de zorginstelling de AS heeft gedelegeerd aan de dienstverlener die de AS opereert.

Oplossing

De zorginstelling maakt een Verifiable Presentation met daarin het ServiceProviderDelegationCredential en het HealthcareProviderCredential. Het HealthcareProviderCredential is nodig zodat de client kan verifieren dat de zorginstelling achter het URA-nummer in de delegatie daadwerkelijk de issuer van de VP is. De audience van deze VP is de issuer identifier van de AS zelf. De AS publiceert deze VP in het OAuth metadata-document onder het veld delegation_presentation.

De client voert de volgende stappen uit voordat het een token request stuurt:

1. Haal het OAuth metadata-document op via RFC 8414 discovery
2. Extraheer de delegation_presentation uit het metadata-document
3. Valideer de VP: controleer de handtekening, audience en geldigheid
4. Controleer dat het HealthcareProviderCredential het URA-nummer bevat dat overeenkomt met het URA in de issuer identifier van de AS
5. Controleer dat het ServiceProviderDelegationCredential in de VP is uitgegeven door de zorginstelling aan de dienstverlener die de AS opereert
6. Pas na succesvolle validatie wordt het token request verstuurd

Dit mechanisme waarborgt dat de client alleen tokens aanvraagt bij een AS die aantoonbaar gemachtigd is door de betreffende zorginstelling (AUTH-024, OAUTH-013).

10.10.6 Access Token request

Het Access token request wordt gestuurd als HTTP POST naar het token endpoint met application/x-www-form-urlencoded encoding.

Parameters:

Parameter	Waarde	Beschrijving

grant_type	urn:ietf:params:oauth:grant-type:jwt-bearer	RFC 7523 grant type
assertion	VP 1 (JWT)	Verifiable Presentation van de zorginstelling met de authorization grant credentials
client_assertion_type	urn:ietf:params:oauth:client-assertion-type:jwt-bearer	RFC 7523 client assertion type
client_assertion	VP 2 (JWT)	Verifiable Presentation van de dienstverlener met de client credentials
scope	string	Use-case scope en resource scopes, spatie-gescheiden

Daarnaast MOET het request een DPoP proof bevatten in de DPoP HTTP header conform RFC 9449. De DPoP proof MOET ondertekend zijn met ES256 (sectie 10.3.3).

Verwerking door de AS

De AS verwerkt het token request in de volgende volgorde (zie ook sectie 8.4.3):

1. Valideer VP 2 (dienstverlener): controleer stelseltoelating via ServiceProviderCredential en delegatie via ServiceProviderDelegationCredential
2. Valideer VP 1 (zorginstelling): controleer identiteit via HealthcareProviderCredential
3. Controleer de use-case scope en bepaal welke aanvullende credentials vereist zijn
4. Valideer de aanvullende credentials (PatientEnrollmentCredential, HealthcareProfessionalDelegationCredential) indien vereist door het autorisatiebeleid
5. Controleer dat de gevraagde resource scopes passen binnen de bevoegdheden uit de credentials
6. Valideer de DPoP proof
7. Geef een access token uit

VP-validatie

Bij de validatie van de VPs in het token request controleert de AS aanvullend:

- De `jti` claim van elke VP MOET uniek zijn. De AS MOET een lijst van ontvangen jti waarden bijhouden binnen de geldigheid van de en VPs met een eerder gebruikte jti weigeren. Dit voorkomt replay attacks.

10.10.7 Access Token response

Bij een succesvol token request retourneert de AS:

```
{
  "access_token": "<opaque token>",
  "token_type": "DPoP",
  "expires_in": 300,
  "scope": "<gehonoreerde scopes>"
}
```

Het access token is opaque: het bevat geen leesbare claims voor de client. De resource server haalt de claims op via token introspectie bij de AS.

Het access token is gebonden aan de DPoP-sleutel (OAUTH-010).

10.10.8 Access Token gebruik

Bij elk verzoek aan de resource server MOET de client het access token en een verse DPoP proof meesturen. De DPoP proof MOET ondertekend zijn met dezelfde sleutel als bij het token request.

Het verzoek aan de resource server bevat:

- De Authorization header met waarde DPoP <access_token>
- De DPoP header met een verse DPoP proof (JWT) conform RFC 9449

De DPoP proof in het resource request MOET de volgende claims bevatten:

- htm: de HTTP-methode van het verzoek (bv. GET)
- htu: de URL van het resource endpoint
- iat: het tijdstip van aanmaak van de proof
- jti: een unieke identifier voor de proof

De resource server MOET controleren dat de DPoP proof geldig is en dat de publieke sleutel in de proof overeenkomt met de cnf claim uit de token introspectie-response (sectie 10.9.9).

10.10.9 Access token validatie door de resource server

Het access token is opaque voor de client, maar de resource server MOET de volgende informatie uit het token kunnen afleiden om het autorisatiebesluit te nemen:

- Of het token actief en niet verlopen is (hele korte levensduur)
- De gehonoreerde scopes
- Het URA-nummer van de zorginstelling
- Aanvullende claims (UZI-nummer, rolcode, BSN) afhankelijk van de use-case scope
- De DPoP key binding (cnf), zodat de RS kan verifiëren dat de DPoP proof bij het resource request is ondertekend met dezelfde DPoP sleutel als waarmee het access token is aangevraagd. (vooralsnog optioneel)

Hoe de RS deze informatie verkrijgt is een implementatiedetail van de AS/RS combinatie. Mogelijke mechanismen zijn:

- **Token introspectie** (RFC 7662): de RS bevraagt het introspectie-endpoint van de AS.
- **Self-contained token**: de AS en RS spreken een token-formaat af dat de RS zelf kan interpreteren (bv. een ondertekende JWT met de claims erin)

Dit stelsel schrijft geen specifiek mechanisme voor. Wel geldt dat ongeacht het gekozen mechanisme, de RS MOET kunnen beschikken over de DPoP key binding om de sender-constrained validatie uit te voeren (OAUTH-010). Deze binding wordt vastgelegd in de cnf claim, die een JWK Thumbprint (jkt) bevat van de publieke sleutel waarmee het token is aangevraagd (zie RFC 9449 sectie 6.1 voor het volledige validatiemechanisme). Bij token introspectie wordt de cnf claim geleverd in de introspectie-response; bij een self-contained token is deze onderdeel van de token payload.

10.10.10 Foutafhandeling

Bij fouten in het token request retourneert de AS een error response conform RFC 6749 sectie 5.2.

Naast de standaard OAuth error codes definieert dit stelsel de volgende aanvullende error codes:

Error code	Beschrijving
invalid_presentation	Een of beide VPs zijn ongeldig (handtekening, structuur, audience)
invalid_credential	Een credential in de VP is ongeldig (verlopen, ingetrokken, issuer niet vertrouwd)
missing_credential	Een credential dat vereist is door het autorisatiebeleid ontbreekt in de VP
insufficient_scope	De gevraagde scope past niet binnen de bevoegdheden uit de credentials
invalid_delegation	De delegatierelatie tussen dienstverlener en zorginstelling is ongeldig of ontbreekt

De error response MOET een error_description veld bevatten met een menselijk leesbare toelichting. De AS MAG GEEN details over de interne autorisatielogica of de inhoud van credentials van de bronhouder opnemen in de error response, om informatielekken te voorkomen.

10.11 Adressering (ntb)

- Mapping van mCSD-resources naar het geharmoniseerde model
- Endpoint-types en payload types
- Relatie Endpoint-resource naar OAuth AS issuer identifier

10.12 Voorbeelden

Deze sectie bevat uitgewerkte voorbeelden van de technische artefacten die in de voorgaande secties zijn gespecificeerd. De voorbeelden gebruiken fictieve maar realistische waarden. Alle sleutelmateriaal is gegenereerd voor dit document en MOET NIET worden gebruikt in productie.

10.12.1 DID-document zorginstelling (did:web)

Het volgende voorbeeld toont het DID-document van een fictieve zorginstelling "Huisartsenpraktijk De Linden" met URA-nummer 12345678. Het document wordt gepubliceerd op https://huisarts-delinden.nl/.well-known/did.json.

Het document bevat twee ECDSA P-256 sleutels (ES256): een voor het ondertekenen van Verifiable Credentials (assertionMethod) en een voor het ondertekenen van Verifiable Presentations (authentication). Conform AUTH-015 zijn deze sleutels verschillend.


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "id": "did:web:huisarts-delinden.nl",
  "verificationMethod": [
    {
      "id": "did:web:huisarts-delinden.nl#assertion-key-1",
      "type": "JsonWebKey2020",
      "controller": "did:web:huisarts-delinden.nl",
      "publicKeyJwk": {
        "kty": "EC",
        "crv": "P-256",
        "x": "f83OJ3D2xF1Bg8vub9tLe1gHMzV76e8Tus9uPHvRVEU",
        "y": "x_FEzRu9m36HLN_tue659LNpXW6pCyStikYjKIWI5a0"
```

```
      }
    },
    {
      "id": "did:web:huisarts-delinden.nl#auth-key-1",
      "type": "JsonWebKey2020",
      "controller": "did:web:huisarts-delinden.nl",
      "publicKeyJwk": {
        "kty": "EC",
        "crv": "P-256",
        "x": "iGRzTt4S5MWRMj9AHYxMj3NY2gczR30YS1YSwNivfbk",
        "y": "L2n3xtAiIfikTAKztVOjvnykGqNPcEWCDAcEMJn3cNo"
      }
    }
  ],
  "assertionMethod": [
    "did:web:huisarts-delinden.nl#assertion-key-1"
  ],
  "authentication": [
    "did:web:huisarts-delinden.nl#auth-key-1"
  ]
}
```

Toelichting:

- De @context bevat de standaard DID-context en de JWS 2020 suite voor JsonWebKey2020 ondersteuning
- Beide sleutels zijn ECDSA P-256, het aanbevolen algoritme uit sectie 10.3.1
- assertionMethod verwijst naar de sleutel waarmee deze zorginstelling credentials kan uitgeven (bv. ServiceProviderDelegationCredential)
- authentication verwijst naar de sleutel waarmee Verifiable Presentations worden ondertekend bij een token request
- Het domein huisarts-delinden.nl voldoet aan de .nl TLD-eis uit sectie 10.3.1

10.12.2 Gedeelde authentication key (sectie 10.7.4)

Het volgende voorbeeld toont hoe een zorginstelling een authentication key deelt met haar dienstverlener, zodat de dienstverlener namens de zorginstelling VPs kan ondertekenen (optie 2 uit sectie 10.7.4).

DID-document dienstverlener (did:web:lsp.nl) -- relevante fragmenten:

```
{
  "id": "did:web:lsp.nl",
  "verificationMethod": [
    {
      "id": "did:web:lsp.nl#auth-key-1",
      "type": "JsonWebKey2020",
      "controller": "did:web:lsp.nl",
      "publicKeyJwk": {
        "kty": "EC",
        "crv": "P-256",
        "x": "2nDYkQgFEn8vEdDaRJZx0ePdqkOvS4ZgDE3pRtK3g4A",
```

```
        "y": "bMzg2nHmWfBJxSDBMOR4FKnMXfG0Ey8yCQOzqaV1bRo"
      }
    }
  ],
  "authentication": [
    "did:web:lsp.nl#auth-key-1"
  ]
}
```

DID-document zorginstelling (did:web:huisarts-delinden.nl) -- relevante fragmenten:

```
{
  "id": "did:web:huisarts-delinden.nl",
  "authentication": [
    "did:web:huisarts-delinden.nl#auth-key-1",
    "did:web:lsp.nl#auth-key-1"
  ]
}
```

Toelichting:

- De authentication van de zorginstelling bevat twee entries: de eigen key en een verwijzing naar de key van de dienstverlener
- De verwijzing did:web:lsp.nl#auth-key-1 is een externe referentie: de verifier resolveert het DID-document van did:web:lsp.nl om de publieke sleutel op te halen
- De dienstverlener kan nu met zijn eigen private key VPs ondertekenen namens de zorginstelling, omdat de signing key voorkomt in de authentication relationship van de zorginstelling
- De verificationMethod en assertionMethod van de zorginstelling blijven ongewijzigd ten opzichte van voorbeeld 10.11.1

10.12.3 PatientEnrollmentCredential (did:x509 issuer)

Het volgende voorbeeld toont een PatientEnrollmentCredential uitgegeven door een zorgverlener met een UZI-zorgverlenerspas (pastype Z). Het credential bewijst dat patient met BSN 999911234 is ingeschreven bij Huisartsenpraktijk De Linden.

JWT header (decoded):

```
{
  "alg": "PS256",
  "typ": "JWT",
  "kid":
"did:x509:0:sha256:YmFzZTY0...dHJ1c3Q=::san:otherName:2.16.528.1.1007.9
9.2110-1-12345678-Z-90001234-01.015-12345678#0",
  "x5c": [
    "MIIFjDCCA3SgAwIBAgIUe8Y...kortLeafCert...==",
    "MIIFcDCCA1igAwIBAgIUa5B...kortIntermediateCert...==",
    "MIIFZDCCAxygAwIBAgIUbGp...kortRootCert...=="
  ],
  "x5t#S256": "dGhpcyBpcyBhIGV4YW1wbGUgdGh1bWJwcmludA"
}
```

JWT payload (decoded):


```
{
  "iss":
"did:x509:0:sha256:YmFzZTY0...dHJ1c3Q=::san:otherName:2.16.528.1.1007.9
9.2110-1-12345678-Z-90001234-01.015-12345678",
  "sub": "did:web:huisarts-delinden.nl",
  "jti": "urn:uuid:a1b2c3d4-e5f6-7890-abcd-ef1234567890",
  "nbf": 1740000000,
  "exp": 1786320000,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "http://gis-nl.example/"
    ],
    "type": [
      "VerifiableCredential",
      "PatientEnrollmentCredential"
    ],
    "issuanceDate": "2025-02-20T00:00:00Z",
    "expirationDate": "2026-08-08T00:00:00Z",
    "credentialSubject": {
      "id": "did:web:huisarts-delinden.nl",
      "@type": "HealthcareProvider",
      "hasEnrollment": {
        "@type": "PatientEnrollment",
        "issuedTo": {
          "@type": "HealthcareProvider",
          "identifier": {
            "@type": "Identifier",
            "system": "http://fhir.nl/fhir/NamingSystem/ura",
            "value": "12345678"
          }
        },
        "patient": {
          "@type": "Patient",
          "identifier": {
            "@type": "Identifier",
            "system": "http://fhir.nl/fhir/NamingSystem/bsn",
            "value": "999911234"
          }
        },
        "enrolledBy": {
          "@type": "HealthcareWorker",
          "identifier": {
            "@type": "Identifier",
            "system": "http://fhir.nl/fhir/NamingSystem/uzi-nr-pers",
            "value": "90001234"
          }
        }
      }
    }
```

```
}
```

Toelichting:

- De alg is PS256 (RSA-PSS), het aanbevolen algoritme voor did:x509 (sectie 10.3.2)
- De x5c header bevat de volledige certificaatketen: leaf-certificaat, intermediate CA en root CA. De verifier gebruikt deze keten om het DID-document te resolveren (sectie 10.4.2)
- De kid bevat de volledige did:x509 identifier met daarin het UZI-nummer (90001234), pastype (Z) en rolcode (01.015) via de san:otherName policy
- De x5t#S256 is de SHA-256 thumbprint van het leaf-certificaat
- De expirationDate ligt binnen 18 maanden na uitgifte, conform het maximale geldigheidsbeleid voor inschrijftokens
- De credentialStatus verwijst naar de status list bij de toolingpartij (sectie 10.8.4)
- De enrolledBy gebruikt type HealthcareWorker (niet HealthcareProfessional), conform sectie 10.6.5
- Het issuedTo veld bevat het URA-nummer van de zorginstelling ten behoeve waarvan de inschrijving is uitgegeven. De verifier controleert dat dit overeenkomt met het URA in het HealthcareProviderCredential in dezelfde VP
- Het credentialSubject bevat geen ura veld: de zorgverlener kan geen claim maken over het URA-nummer van de zorginstelling. De binding tussen did:web en URA wordt vastgesteld via het HealthcareProviderCredential dat in dezelfde VP wordt gepresenteerd

10.12.4 ServiceProviderDelegationCredential (did:web issuer)

Het volgende voorbeeld toont een ServiceProviderDelegationCredential uitgegeven door Huisartsenpraktijk De Linden aan dienstverlener LSP. Het credential bewijst dat de zorginstelling het LSP machtigt om namens haar op te treden.

JWT header (decoded):

```
{
  "alg": "ES256",
  "typ": "JWT",
  "kid": "did:web:huisarts-delinden.nl#assertion-key-1"
}
```

JWT payload (decoded):

```
{
  "iss": "did:web:huisarts-delinden.nl",
  "sub": "did:web:lsp.nl",
  "jti": "urn:uuid:b2c3d4e5-f6a7-8901-bcde-f23456789012",
  "nbf": 1740000000,
  "exp": 1771536000,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "http://gis-nl.example/"
    ],
    "type": [
      "VerifiableCredential",
      "ServiceProviderDelegationCredential"
    ],
```

```
    "issuanceDate": "2025-02-20T00:00:00Z",
    "expirationDate": "2026-02-20T00:00:00Z",
    "credentialSubject": {
      "id": "did:web:lsp.nl",
      "@type": "ServiceProvider",
      "hasDelegation": {
        "@type": "Delegation",
        "delegatedBy": {
          "@type": "HealthcareProvider",
          "identifier": {
            "@type": "Identifier",
            "system": "http://fhir.nl/fhir/NamingSystem/ura",
            "value": "12345678"
          }
        },
        "scope": {
          "@type": "DelegationScope",
          "authorizationRule": "urn:gis-nl:authorization-
rule:medicatie",
          "authorizedActions": [
            "patient/MedicationRequest.read",
            "patient/MedicationDispense.read"
          ]
        }
      }
    }
  }
}
```

Toelichting:

- De alg is ES256 (ECDSA P-256), het aanbevolen algoritme voor did:web (sectie 10.3.1)
- De kid verwijst naar de assertion key uit het DID-document van de zorginstelling (voorbeeld 10.11.1). De verifier resolveert dit DID-document en controleert dat de key voorkomt in assertionMethod
- Er is geen x5c header: bij did:web wordt het sleutelmateriaal opgehaald uit het DID-document, niet uit een certificaatketen
- Het iss is de did:web van de zorginstelling, het sub is de did:web van de dienstverlener
- De authorizedActions bevatten SMART-on-FHIR scopes als voorbeeld; de definitieve waarden hangen af van de scope-architectuur (OV-012, OV-013)
- De verifier controleert dat de authorizedActions een subset zijn van de services in het ServiceProviderCredential van het LSP (sectie 10.6.7)

10.12.5 Token request (RFC 7523)

Het volgende voorbeeld toont de volledige HTTP-interactie bij een token request. Het LSP (did:web:lsp.nl) vraagt namens Huisartsenpraktijk De Linden een access token aan bij de authorization server van de bronhouder.

DPoP wordt in dit voorbeeld buiten beschouwing gelaten. In productie MOET elke token request een DPoP proof bevatten (sectie 10.9.6).

Stap 1: Discovery

De client zoekt eerst de AS identifier op in een vertrouwde tabel of adreseringsfunctie en leidt daar het metadata endpoint uit af om deze vervolgens op te halen.

In het metadata document staat het token endoint wat gebruikt kan worden voor het token request.

Request:

```
GET /.well-known/oauth-authorization-server/ura/87654321 HTTP/1.1
Host: as.bronhouder-xyz.nl
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "issuer": "https://as.bronhouder-xyz.nl/ura/87654321",
  "token_endpoint": "https://as.bronhouder-xyz.nl/ura/87654321/token",
  "grant_types_supported": [
    "urn:ietf:params:oauth:grant-type:jwt-bearer"
  ],
  "token_endpoint_auth_methods_supported": [
    "private_key_jwt"
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
    "ES256", "ES384", "ES512", "PS256"
  ],
  "dpop_signing_alg_values_supported": [
    "ES256"
  ]
}
```

De AS metadata bevat in productie ook de velden delegation_presentation en provider_presentation (sectie 10.9.5). Deze zijn in dit voorbeeld weggelaten omdat de specificatie van deze presentations nog niet volledig is uitgewerkt.

Stap 2: Token request

De client stelt twee VPs samen en verstuurt ze in het token request.

VP 1 -- Zorginstelling (JWT header, decoded):

```
{
  "alg": "ES256",
  "typ": "JWT",
  "kid": "did:web:huisarts-delinden.nl#auth-key-1"
}
```

VP 1 -- Zorginstelling (JWT payload, decoded):

```
{
  "iss": "did:web:huisarts-delinden.nl",
  "aud": "https://as.bronhouder-xyz.nl/ura/87654321",
  "jti": "urn:uuid:c3d4e5f6-a7b8-9012-cdef-345678901234",
  "exp": 1740000300,
  "vp": {
    "@context": ["https://www.w3.org/2018/credentials/v1"],
    "type": ["VerifiablePresentation"],
    "verifiableCredential": [
      "eyJhbGciOiJQUzI1NiIs...kort HealthcareProviderCredential....",

"eyJhbGciOiJQUzI1NiIs...kortHealthcareProfessionalDelegationCredential.
...",
      "eyJhbGciOiJQUzI1NiIs...kortPatientEnrollmentCredential...."
    ]
  }
}
```

VP 2 -- Dienstverlener (JWT header, decoded):

```
{
  "alg": "ES256",
  "typ": "JWT",
  "kid": "did:web:lsp.nl#auth-key-1"
}
```

VP 2 -- Dienstverlener (JWT payload, decoded):

```
{
  "iss": "did:web:lsp.nl",
  "aud": "https://as.bronhouder-xyz.nl/ura/87654321",
  "jti": "urn:uuid:d4e5f6a7-b8c9-0123-defa-456789012345",
  "iat": 1740000300,
  "exp": 1740000310,
  "nbf": 1740000300,
  "vp": {
    "@context": ["https://www.w3.org/2018/credentials/v1"],
    "type": ["VerifiablePresentation"],
    "verifiableCredential": [
      "eyJhbGciOiJFUzI1NiIs...kortServiceProviderCredential....",

"eyJhbGciOiJFUzI1NiIs...kortServiceProviderDelegationCredential...."
    ]
  }
}
```

Stap 3: Token request verzenden

De twee VPs worden als JWT-encoded strings verstuurd in het token request.

Request:

```
POST /ura/87654321/token HTTP/1.1
Host: as.bronhouder-xyz.nl
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
&assertion=eyJhbGciOiJFUzI1NiIs...kortVP1zorginstelling....
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer
&client_assertion=eyJhbGciOiJFUzI1NiIs...kortVP2dienstverlener....
&scope=usecase%3Amedicatie%20patient%2FMedicationRequest.read%20patient
%2FMedicationDispense.read
```

Stap 4: Token response

Response (succes):

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "access_token": "opaque-token-a1b2c3d4e5f6",
  "token_type": "Bearer",
  "expires_in": 300,
  "scope": "usecase:medicatie patient/MedicationRequest.read
patient/MedicationDispense.read"
}
```

Response (fout):

```
HTTP/1.1 400 Bad Request
Content-Type: application/json

{
  "error": "missing_credential",
  "error_description": "The required PatientEnrollmentCredential is
missing from the presentation"
}
```

Toelichting:

- De aud in beide VPs is de issuer identifier van de AS, niet de URL van het token endpoint
- Elke VP heeft een unieke jti en een korte exp (in dit voorbeeld 5 minuten). De AS houdt gebruikte jti waarden bij binnen dit tijdvenster om replay attacks te voorkomen (sectie 10.9.6)
- VP 1 is ondertekend met de authentication key van de zorginstelling; VP 2 met de authentication key van de dienstverlener
- De credentials in verifiableCredential zijn zelf ook JWTs, waardoor het geneste JWT-in-JWT structuren zijn. De buitenste JWT (VP) en binnenste JWTs (VCs) worden onafhankelijk gevalideerd
- Het token_type is Bearer. In productie wordt DPoP gebruikt (sectie 10.9.6), wat het token type wijzigt naar DPoP en extra proof-headers vereist bij elk resource request

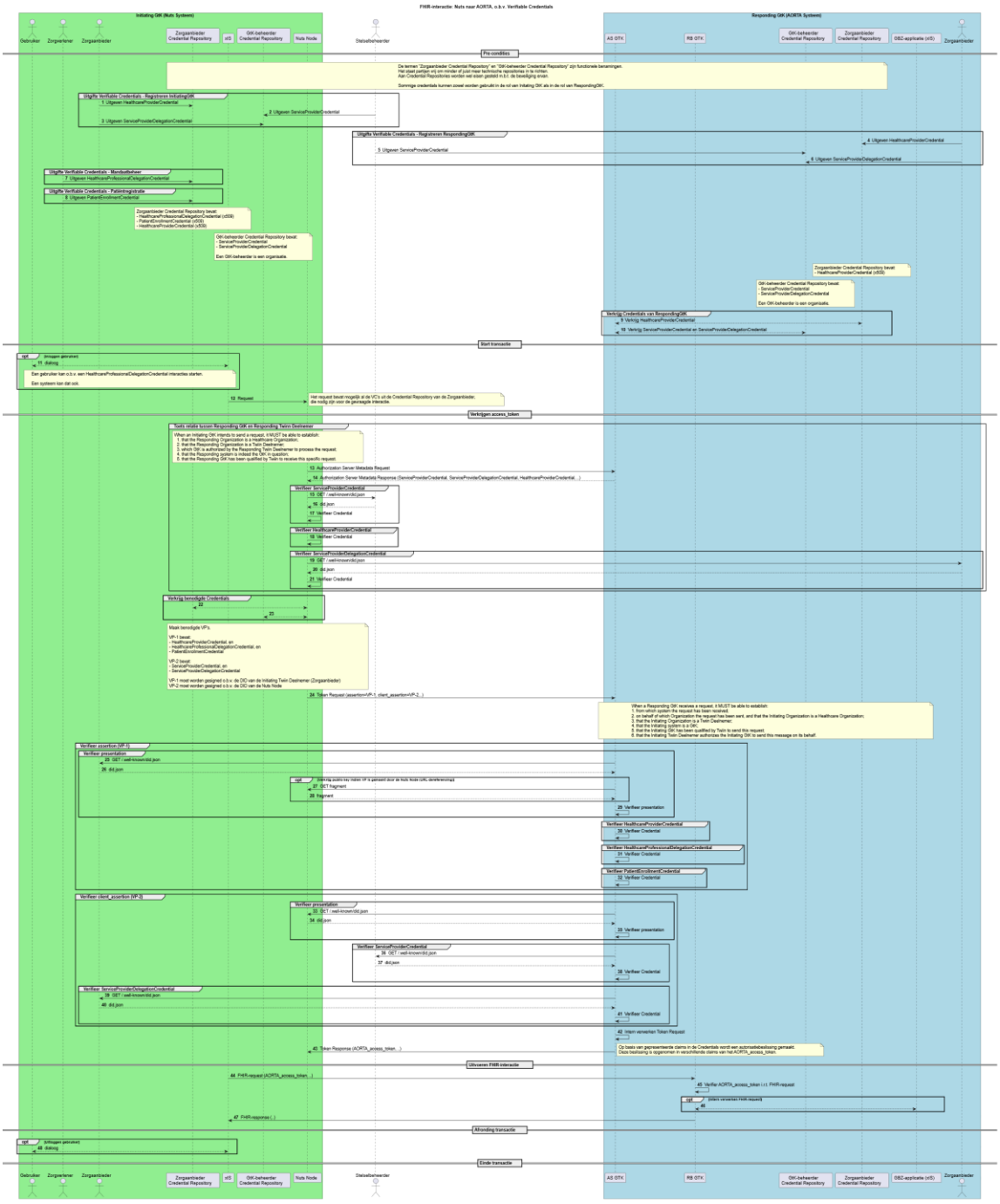
11 Bijlage 2: Visualisaties Overzicht

11.1 FHIR-interactie: Nuts naar AORTA obv Verifiable Credentials

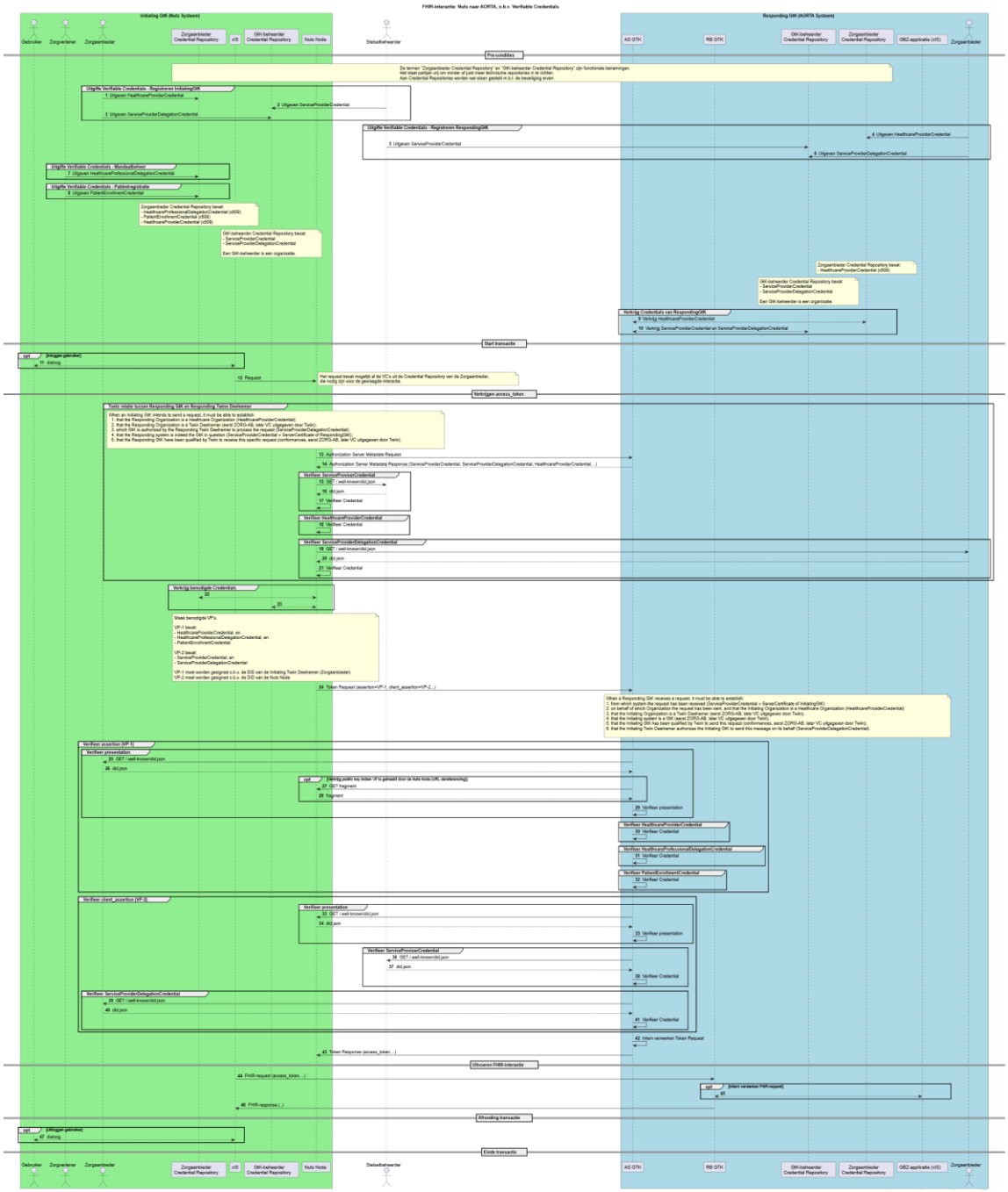
The high-level flow of requests and information is shown in the picture below.

Link naar flow om in browser te kopiëren (link is te lang voor een koppeling in Word):

https://www.planttext.com/?text=rLdjRXit5lslfxZm_gWDI6hYrEdMMnTrcgnhj6aCsqc1Oe606j4ZMZEaIb9oubVQn-YBxRdaV4eZMNAC1GhuXonUtc-UUqZzwBomVfvdFJ7tHi_paRIzdbS-axJtxv_FBmTAUsb5ufKyfj_ctf4MmjBfkylhqpwPuMYu6D87QTMD4YDi-idAiTHUYSpjzTnKwPcm8gTNvjE568-LJkdeMQ_N6vbFj7Uk5GGzVtdcVw7zeFxgi_DIvWTxz8zVLJhnPrPAtIE22yRItfaSsRcQIhj7mf5AHsJiM5fwNelyOMowa3QJkfIwNnHIXsqf8VH8mTzIJ1HYBtgGW-DU9Mecj5-Ifl_eEaowb3FZ57H-BhNSbJuzMrQ3C0SZEP7IFgWc7LLgNgwuy-dyAafzKgwKEbeM2kdypOnb5DNuLARXMK_gCQ48HIKkfPiPFQug4SgxKefNsLnkIg2j4lZFvoikdxtwOo1ciqmbgBYaVOHm47VLCNoxah3JApgx_YN8YTHF2xcZ5RdBLvMSRSWTVK4XRLt8brzGI5iNykYxEkr54g-yp9pCAbLXY_EZITc9E2md9tHXvI3X0Y5rZavEUZrjFAg9DWyDrsTduUDhIJYjkTJBWQxnZmNReQmHl5Utccxc6ZXWjCGv7qajSIIBr4FO_LbwU2s4ZrcwXTw5LRTaSe8GwpKtT3jNpbCEGt0ocMZbaeaaMrhXo9J64bcLJ7nKV2fqfqiiVCSfqdGdCvBAuLCgqQ_Pc7AWaX_IcBrSI9Mfb1jRseK8El5tPV9SfPAI6greEjSQIkuDAonqfn5jF3i6TTPa12N4m5NZ5czkhzV72Ul3K7IkLw-NMZEVqNlbKtM3GBjnamPGa29NLbePZKMKX3BupZ0r-26K_JYeGemQ5H2PdoJ2oWjh5WefhpLYKsWfteLkREowGb9KqhsbjBDnnslqGYguAHfxETuGwUC2RcKFZjZeY7rKm7RxW4ix_vU0tmezndc91ozaU_5GLM-aSx0higVouG8w_lglHjf3yXcNrth2ijZvHgF7Cm2CxpRTXYLesmA6-9GAVmpXmGu1Ou8SFVlk8EpQu5nJR5FBb7BLMMr4WeR0_YrmiXd9favRMUsiA0FL6wI-RHZ34eI8EAr0K0wy2J2rr_RByxzzYkpVA4NnTE1GJ36XqjQHMC5kPZjC9xuVL01KRNm0W1hx0g1K-zP6JRkZ3QZ15HDumkdLBh3qm0xCp6DkP2PDwo4MOGQ4EJZ5pF6Onj1dJ8g5LhltUHLVnkHM-scA_1IKN-w4JbJV8fZUmECutiCmZbPS99l1nXX4mfWfIrHrmuTUB_1Tzfx9x35gzUSSCpysecMAMd0H6nTYir5kKfcfsoacDK_f3pzzvMYkF7_kxb7k0oospawVNHqZlp2jqaY85WOS3eA0I2j4YazrdCsMGvdAyYDIaIJ8rKTlflY7gnKxyjf8y7Khiy2F_TovrYmCLAFzpVMTqXgSJsPQvg6yZIeYK_sOfv3YtoTikSacWaBsLuyTUKEE_HLbwh3NqzltLzV88ONP0H5yZu_AJOw3JgBdG_8JPDY3o3KSUnTEtdre0ZwDej4ghSL_5NeEjzM3a5KZv7B_Yo7TJS0QOqmGdFi9IEAz1DI-lAnrIGS7DhE6Qn8aYmIKgh_fTYsqQywscD_23g_7Z5BOtuZkg5i5Iqz0zqTyblwSYmnJEZeSFOHVLYPIBP3x2GovcKmWafGUjeu75HSy70v6dcCwBL8GayUuWb3VIYzmk4HrSWgS6jHdwg5zxBx3_MqjZFMt0R7-HlZiqt1um5Ut2givDV1ZqyHeP839tp6TlRcchuTWyzbWgisT_dginiDRPtGGZWInZhkrM6ag5ciFMYORIBpgwmFpuMcCR3KacxOmn1xAJE31JvMO5LfQpK7S81b9Mo3igZwEGuedxj9NF4pNCCuMvBqLOjgmyU7YApVa37wu63pVbl7qAJmzxK9BgosR27Dqut0hBbGftAxKPOGvfabzYtKgrO2MOdOZ7Q_FNvTJhZ4Hbf5nlpK13qgtjzTTFK4rXk4IJbs7CLZW4UqBZ3tBKPrm67rACixYnzRNXts6XxhmhAXl8sM9SsuPPWiSTRlCDyos6sloOh0KUDyO43Ls5zh7ZFUOP81DS56HtV2ZHzpT6cITEZ1zuHCkXVMeQ1Hcfu7wOhYbZevX-atttdhQ2SudInvrIsunr0BH21EjCMfVTgjRxiXgiBikmotbEOwfI2MNGtbNbAJp8b0WMDLZjC-zTz01jpChkL0XXm4Fu_GCIFKGhAe2LcFRjvQOhbUuE9kZ1HEQoizCBT3zE7IS-LJcW3Imre9qLcUBzjzV_Zh00PKt_7wI81i71VEet8jepGxUM94o71KInMci_6ejC-TkgeaYQzDHe_8Zfk4w6slcoWCMDh-LF8czJG3_20DTWxBOiOo1eJyFT-lFkW4sTEXIBxGMdw07DhEtqi1Ev6q7HxSkxBQSwcdE_kFRfBtpd6-Uk99AUmSa0Mgq1cjlgH7AnPBDXnzyFZPlff63jsxMxsOq4ax5Tv9K5fKFZoxeKQ7oyXsy-QR2FC67vmB-XT76zvYHT1YpZd6xWBLX-FNYdf_igoN-NMY66xFX7pHKYCqb4vLbI49baNsPW8-iHh1q0t-l_CA41-QbtpN37RnyMR0XcK6YdD5haqFnjwPgLr4ys-4BgQ7btoIQYejNcgMojIGA2_4PYLzimZD8QJM-uHGRoag6cnF2FGLvYGIeusq8kTZ-SIYylB3ADtpLNLRt8vRdUVO_


FHIR-interactie: Nuts naar AORTA, o.b.v. Verifiable Credentials
Initiating GIK (Nuts Systems)
Responding GIK (AORTA Systems)
Gebruiker
Zorgverlener
Zorgaanbieder
Zorgaanbieder Credential Repository
eIS
GIK-beheerder Credential Repository
Nuts Node
Statusbeheerder
AS GTK
RS GTK
OBZ-applicatie (eIS)
Pre-condities
Uitgifte Verifiable Credentials - Registreren InitiatingGIK
Uitgifte Verifiable Credentials - Registreren RespondingGIK
Uitgifte Verifiable Credentials - Mandaatbeheer
Uitgifte Verifiable Credentials - Patiëntinschrijving
Verkrijg Credentials van RespondingGIK
Start transactie
Verkrijgen access_token
Verkrijg benodigde Credentials
Verifier assertion (VP-1)
Verifier client_assertion (VP-2)
Uitvoeren FHIR-interactie
Afronding transactie
Einde transactie

Vorig versie:



12 Bijlage 3 – RFC's en standaarden voor Best Practices Security

12.1 Identity & Access Management

Domein	RFC / standaard	Beschrijving
OAuth 2.0 Core	**RFC 6749**	Definieert het OAuth 2.0 framework voor gedelegeerde autorisatie, inclusief rollen, grant flows, access tokens en token-endpoints.
PKCE	**RFC 7636**	Beschrijft Proof Key for Code Exchange (PKCE), waarmee onderschepping van authorization codes wordt voorkomen via een cryptografische challenge/verifier mechanisme.
JWT Bearer Flow	**RFC 7523**	Definieert hoe JWT's gebruikt kunnen worden als bearer assertion voor OAuth 2.0 client-authenticatie en tokenaanvragen.
OAuth 2.0 Mutual TLS	**RFC 8705**	Beschrijft client-authenticatie met mutual TLS en het cryptografisch binden van tokens aan X.509-certificaten (sender constrained tokens).
JWT Profile for OAuth Access Tokens	**RFC 9068**	Standaardiseert het gebruik van JWT access tokens binnen OAuth 2.0 inclusief claims en validatieregels.
OID	**OpenID Connect 1.0 / ISO 26131:2024**	Voegt een identiteitslaag toe bovenop OAuth 2.0 waarmee gebruikersauthenticatie en gestandaardiseerde identity claims mogelijk worden.
Authorization Server Metadata	**RFC 8414**	Definieert een metadataformaat waarmee OAuth/OIDC clients automatisch configuratie-informatie van authorization servers kunnen ophalen.
Pushed Authorization Requests	**RFC 9126**	Definieert Pushed Authorization Requests waarmee authorization requests beveiligd rechtstreeks tussen client en authorization server worden uitgewisseld.
JWT Authorization Requests	**RFC 9101**	Beschrijft JWT Secured Authorization Requests waarmee authorization requests cryptografisch beschermd worden tegen manipulatie.
Best practices OAuth 2.0	**RFC 9700**	Beschrijft actuele best practices voor veilige OAuth 2.0 implementaties inclusief PKCE, sender-constrained tokens en replaypreventie.

12.2 Verifiable Credentials & Decentralized Identity

Domein	Specificatie	Beschrijving
VC Data Model	**W3C Verifiable Credentials Data Model 1.1**	Definieert het kernmodel, de semantiek en lifecycle van verifieerbare digitale credentials.
VC Overzicht	**Verifiable Credentials Overview**	Geeft een overzicht van het VC-ecosysteem voor cryptografisch verifieerbare digitale verklaringen.

VC Presentatie	**W3C VC-JOSE-COSE**	Beschrijft hoe Verifiable Credentials worden gerepresenteerd met JWT/JWS of COSE-gebaseerde cryptografie.
OID VC Issuance	**OpenID for Verifiable Credential Issuance**	Definieert een OAuth/OIDC-gebaseerd protocol voor veilige uitgifte van Verifiable Credentials aan wallets.
DID Core	**W3C DID Core 1.0**	Definieert de syntaxis en resolutiemechanismen van Decentralized Identifiers (DID's).
DID Web	**did:web**	DID-methode waarbij publieke sleutels en metadata via HTTPS en well-known locaties worden gepubliceerd.
DID x509	**did:x509**	DID-methode waarbij identiteiten worden afgeleid uit X.509 certificaatketens.
X509Credential	**RFC023**	Beschrijft binnen het Nuts-netwerk hoe X.509-certificaten gekoppeld worden aan Verifiable Credentials en DID-identiteiten.

12.3 Transport & Network Security

Domein	RFC	Beschrijving
TLS 1.3	**RFC 8446**	Definieert TLS 1.3 voor versleutelde en integere netwerkcommunicatie met moderne cryptografische algoritmen.
X.509 Certificaten	**RFC 5280**	Beschrijft het internetprofiel voor X.509-certificaten en certificaatketenvalidatie inclusief CRL's.
Service Identificatie	**RFC 6125**	Definieert hostname-verificatie voor TLS-verbindingen ter voorkoming van man-in-the-middle-aanvallen.
TLS best practices	**RFC 9325**	Geeft actuele beveiligingsrichtlijnen voor veilig gebruik van TLS en cryptografische configuraties.
mTLS	**RFC 8705**	Beschrijft mutual TLS voor client-authenticatie en sender-constrained OAuth tokens.

12.4 Token Security & Cryptography

Domein	RFC	Beschrijving
JSON Web Signature (JWS)	**RFC 7515**	Definieert digitale handtekeningen voor JSON-gebaseerde berichten en tokens.
JSON Web Encryption (JWE)	**RFC 7516**	Definieert encryptie van JSON-gebaseerde berichten en tokens.
JSON Web Key (JWK)	**RFC 7517**	Definieert een JSON-formaat voor cryptografische sleutels en sleutelsets.
JSON Web Algorithms (JWA)	**RFC 7518**	Definieert cryptografische algoritmen voor JWS, JWE en JWK.
JSON Web Token (JWT)	**RFC 7519**	Definieert een compacte JSON-gebaseerde tokenstandaard voor claimsuitwisseling.

Proof-of-Possession Key Semantics	**RFC 7800**	Beschrijft hoe een JWT cryptografisch gekoppeld wordt aan een specifieke sleutelhouder.
Demo Proof-of-Possession Key Semantics (DPoP)	**RFC 9449**	Definieert Demonstrating Proof-of-Possession waarmee OAuth tokens sender-constrained worden gemaakt.
Bearer Token Usage	**RFC 6750**	Beschrijft het gebruik van bearer tokens voor toegang tot OAuth protected resources.
JWT Access Tokens	**RFC 9068**	Standaardiseert het gebruik van JWT-gebaseerde OAuth access tokens.

12.5 Token Lifecycle & Authorization Operations

Domein	RFC	Beschrijving
Token Revocation	**RFC 7009**	Definieert een endpoint waarmee OAuth tokens ongeldig kunnen worden gemaakt.
Token Introspection	**RFC 7662**	Definieert een mechanisme waarmee resource servers de status en metadata van OAuth tokens kunnen opvragen.
Token Exchange	**RFC 8693**	Beschrijft een protocol voor het uitwisselen van security tokens tussen systemen.
Online Certificate Status Protocol (OCSP)	**RFC 6960**	Definieert een protocol voor realtime controle van certificaatstatussen.
Certificate Revocation Lists (CRL)	**RFC 5280**	Beschrijft Certificate Revocation Lists voor het intrekken van certificaten.

12.6 Trust, Federation & Discovery

Domein	RFC / standaard	Beschrijving
Authorization Server Metadata	**RFC 8414**	Definieert metadata discovery voor OAuth/OIDC authorization servers.
DID Core	**W3C DID Core**	Definieert trustmodellen en sleutelresolutie voor gedecentraliseerde identiteiten.
DID Web	**did:web**	Beschrijft trust via HTTPS-gebaseerde DID publicatie.
DID x509	**did:x509**	Beschrijft trust op basis van bestaande PKI-certificaatketens.
Holder-of-Key	**RFC 7800**	Definieert cryptografisch bewijs van sleutelbezit binnen tokens.
X509Credential	**RFC 023**	Verbindt traditionele PKI met DID- en VC-gebaseerde trustmodellen.
VC Data Model	**VC Data Model**	Definieert trust- en verificatieregels voor digitale credentials.

12.7 Logging, Audit & Accountability

Domein	RFC / standaard	Beschrijving
HTTP Semantics	**RFC 9110**	Definieert HTTP-semantiek inclusief request/response gedrag, methodes en statuscodes.
AuditEvent	**HL7 FHIR R4 Resource**	Definieert een gestandaardiseerd auditlogmodel voor zorggerelateerde security- en transactielogging.
Logging Medische Informatie	**NEN7513**	Beschrijft loggingvereisten voor medische gegevensuitwisseling en zorgtransacties.

12.8 Privacy, Compliance & Governance

Domein	Norm / richtlijn	Beschrijving
Privacy	**AVG/GDPR**	Europese privacywetgeving voor bescherming van persoonsgegevens.
Identificatie en vertrouwensdiensten	**eIDAS**	Europees raamwerk voor elektronische identificatie en vertrouwensdiensten.
Informatiebeveiliging	**NEN7510**	Nederlandse norm voor informatiebeveiliging in de zorg.
Veilige uitwisseling	**NEN7512**	Norm voor veilige uitwisseling van gezondheidsinformatie.
Standaard ISMS	**ISO27001**	Internationale standaard voor Information Security Management Systems (ISMS).
Securityrichtlijnen	**NIST-richtlijnen**	Securityrichtlijnen en best practices voor cybersecurity en risicoanalyse.

12.9 Security Best Current Practices

Domein	Norm / richtlijn	Beschrijving
OAuth beveiligingrichtlijnen	**RFC 9700**	Bundelt actuele beveiligingsrichtlijnen voor OAuth 2.0 implementaties.
Best practices voor TLS	**RFC 9325**	Beschrijft actuele best practices voor veilige TLS-configuraties.

12.10 Operational Security Best Practices

Onderwerp	RFC/ Norm / richtlijn	Beschrijving	Prioriteit & Status
Nonce verplichting	RFC 6749 (OAuth 2.0), OpenID Connect Core 1.0, RFC 8725 (JWT Best Current Practices)	Voorkomt replay attacks door requests uniek en tijdelijk geldig te maken.	**Hoog** • Nog niet expliciet uitgewerkt, maar noodzakelijk voor VC/VP-presentaties en OAuth-transacties.
JTI uniqueness	RFC 7519 (JSON Web Token – `jti` claim)	Voorkomt hergebruik van JWT's via unieke token-identificatie.	**Hoog** • Nog niet expliciet benoemd in document.

One-time-use tokens	RFC 9700 (OAuth 2.0 Security Best Current Practice), RFC 7009 (OAuth 2.0 Token Revocation)	Beperkt tokens tot eenmalig gebruik voor kritieke transacties.	**Hoog** • Nog conceptueel; nog geen concrete lifecycle-afspraken.
Audience restriction	RFC 7519 (aud claim), RFC 9068 (JWT Profile for OAuth 2.0 Access Tokens)	Beperkt tokens tot expliciet toegestane ontvangers.	**Hoog** • Gedeeltelijk aanwezig via endpoint- en GtK-validatie.
Sender-constrained tokens	RFC 8705 (OAuth 2.0 Mutual TLS Client Authentication), RFC 9449 (DPoP), RFC 8446 (TLS 1.3)	Bindt tokens cryptografisch aan clientcertificaten of sleutels.	**Zeer hoog** • Sterk aanwezig in ontwerp via mutual TLS, PKI en VC/VP cryptografie.
Short-lived access tokens	RFC 9700 (OAuth 2.0 Security BCP), RFC 8725 (JWT BCP)	Minimaliseert impact van tokencompromittering door korte geldigheidsduur.	**Hoog** • Nog niet expliciet uitgewerkt.
Key rotation	RFC 7517 (JSON Web Key), RFC 7518 (JSON Web Algorithms), NEN 7510	Verplicht periodieke vervanging van signing keys en certificaten.	**Hoog** • PKI en certificaten aanwezig; rotatiebeleid ontbreekt nog.
Replay detection	RFC 9700 (OAuth 2.0 Security BCP), RFC 9449 (DPoP)	Detecteert hergebruik van requests of tokens.	**Hoog** • Impliciet aanwezig via logging en transaction binding, nog niet expliciet als requirement.
Rate limiting	RFC 9110 (HTTP Semantics), OWASP API Security Top 10 API4, NIS2	Beschermt API's tegen overbelasting en misbruik.	**Midden** • Nauwelijks uitgewerkt; monitoring wel genoemd.
Input validation	RFC 8259 (JSON), OWASP ASVS	Voorkomt injectieaanvallen en malformed requests.	**Hoog** • Nog niet expliciet benoemd.
Immutable audit logging	NEN 7513, RFC 5424 (Syslog Protocol), Wabvpz	Zorgt dat auditlogs niet ongemerkt gewijzigd kunnen worden.	**Hoog** • Nog niet uitgewerkt
Correlation IDs	NEN 7513, RFC 5424 (Syslog Protocol), W3C Trace Context Recommendation	Ondersteunt end-to-end traceability van transacties.	**Hoog** • Deels aanwezig via interactionId/messageId concepten
Scope minimization / Least privilege	RFC 6749, RFC 9396 (OAuth Rich Authorization Requests), OWASP ASVS	Tokens mogen alleen minimale rechten bevatten die nodig zijn voor de transactie.	**Zeer hoog** • Gedeeltelijk aanwezig via autorisatierichtlijnen, nog niet expliciet technisch afgedwongen.
Token introspection	RFC 7662	Real-time controle of tokens nog geldig, actief of ingetrokken zijn.	**Hoog** • Nog niet uitgewerkt.
Token revocation	RFC 7009	Intrekken van gecompromitteerde of verlopen credentials/tokens.	**Hoog** • Nog beperkt uitgewerkt buiten certificaat-intrekking.

PKCE verplichting	RFC 7636	Beschermt authorization codes tegen onderschepping.	**Hoog** • Nog niet expliciet genoemd; relevant bij OAuth gebaseerde flows.
Certificate pinning / trust anchoring	RFC 5280, PKIoverheid CPS	Beschermt tegen rogue CA's en MITM-aanvallen.	**Hoog** • Impliciet aanwezig via PKI/UZI-certificaten.
Secrets management	OWASP Secrets Management Cheat Sheet, NEN 7510	Veilig beheer van signing keys, client secrets en API keys.	**Zeer hoog** • Nog nauwelijks uitgewerkt.
API schema validation	OpenAPI, OWASP API Security Top 10	Controle op payloadstructuur en datatype-validatie.	**Hoog** • Nog niet expliciet opgenomen.
Zero Trust principes	NIST SP 800-207	Geen impliciet vertrouwen tussen infrastructuren; alles expliciet verifiëren.	**Zeer hoog** • Architectuur beweegt hier al sterk naartoe via VC/VP en GtK.
Privacy by design	AVG art. 25, NEN 7510	Minimalisatie van persoonsgegevens en pseudonimisering waar mogelijk.	**Zeer hoog** • Sterk aanwezig vanuit zorgwetgeving, maar technisch nog beperkt uitgewerkt.
Consent integrity validation	Wabvpz, Mitz-afspraken	Controle dat toestemming authentiek, actueel en onveranderd is.	**Zeer hoog** • Toestemming benoemd, maar integriteitscontrole nog niet expliciet.
Immutable event signing	RFC 5848 (Signed Syslog)	Cryptografisch aantonen dat logs niet gewijzigd zijn.	**Hoog** • Mooie aanvulling op NEN7513 logging.
Device attestation	WebAuthn, Android/iOS attestation	Valideert of device betrouwbaar en niet gecompromitteerd is.	**Midden/Hoog** • Relevant richting mobiele DEZI-toekomst.

Note:

De huidige beschreven architectuur introduceert aanzienlijke complexiteit (*dubbele asserties*, embedded VP's, DID-resolutie, credential status checks, DPoP, afhankelijkheid van trust frameworks) vergeleken met een traditioneel en bewezen RFC7523 JWT bearer model. Hoewel als reden wordt gegeven dat private keys niet gedeeld hoeven te worden en autoritatieve registers worden gebruikt, moet de AS nog steeds vertrouwen op de issuer en diens signing keys.

Tot slot is het embedden van VP's in RFC7523 JWT bearer-grants niet de gebruikelijke presentatievorm binnen wallet-ecosystemen; OpenID4VP definieert gestandaardiseerde presentatieflows en transportpatronen voor VP's. De beschreven architectuur is daarom een niet-standaard combinatie van standaarden en zou niet automatisch worden geacht de security-modellen van OpenID4VP over te nemen.

Er is echt meer aanvullende normatieve security guidance en testmateriaal nodig om conformiteit te borgen.

13 Begrippenlijst

Begrip	Omschrijving	Gebruik binnen Project/ Stelsel
Autoritatieve bron	Vertrouwde bron erkend als uitgever van attributen of claims.	Claims op basis van X.509-certificaten van UZI-register en PKIo worden geaccepteerd. Verifiable Credentials (VCs) zijn de technische invulling van deze waarborgen.
GtK (Gekwalificeerd Twiin Knooppunt)	Een gekwalificeerd knooppunt binnen het Twiin afsprakenstelsel dat functioneert als autoritatieve gateway.	Waar beschikbaar worden Twiin-eisen gehanteerd, aangevuld met technische voorzieningen om de vertrouwensketen te borgen.
Knooppunt	Conceptueel punt dat afsprakenstelsels met elkaar verbindt; fungeert als gateway naar andere stelsels.	Wordt ingevuld door concept-GtK's; knooppunten publiceren endpoints van aangesloten zorginstellingen en aggregeren directories.
Zorginstelling	Organisatie die zorg levert, geïdentificeerd door een URA-nummer.	Wordt beschreven in HealthcareProviderCredential; endpoints en inschrijvingen worden via knooppunten gepubliceerd.
Resource Server (RS)	Applicatie of service die toegang tot data verleent op basis van geldige tokens en credentials.	Valideert access tokens, controleert claims voor autorisatiebeslissingen; kan DPoP binding controleren.
Authorization Server (AS)	Verstrekt access tokens op basis van geldige authenticatie en credentials van de client.	Publiceert metadata (.well-known) inclusief delegatie-Verifiable Presentations (VP's); bindt tokens aan audience.
Verifiable Credential (VC)	Digitaal, cryptografisch ondertekend attest van een autoritatieve bron over een subject.	Wordt gebruikt om identiteit, attributen of bevoegdheden van een subject te bewijzen; kan opgenomen worden in VPs.
Verifiable Presentation (VP)	Door de holder ondertekend pakket van één of meerdere VCs.	Bewijst aan een verifier dat de holder beschikt over de juiste credentials; gebonden aan een specifieke audience (aud claim).
DID (Decentralized Identifier)	Unieke, resolvable identifier voor een subject.	Wordt gebruikt in VCs en VPs om issuer en subject te identificeren; sleutelmateriaal wordt gepubliceerd in het DID-document.
LRZa (Landelijk Register Zorgaanbieders)	Root Administration Directory voor zorginstellingen.	Zorginstellingen registreren endpoints van hun Administration Directory; Update Clients gebruiken LRZa om directories te aggregeren in Query Directories.
Administration Directory	Lokaal register van endpoints van zorginstellingen per knooppunt.	Wordt gepubliceerd door Nuts-knooppunten of LSP; biedt overzicht van services en endpoints van aangesloten zorginstellingen.
Query Directory	Geaggregeerde view van meerdere Administration Directories.	Gebruikt door zoekende systemen om endpoints te vinden op basis van URA, diensttype of datatype; kan meerdere endpoints voor dezelfde zorginstelling bevatten.

DPoP key / binding	Sleutel gebruikt om access tokens te binden aan een sessie of request.	Gebruikt door OAuth clients en RS om token misuse te voorkomen; bevestigd via cnf claim.
Trust anchor	Vertrouwde root CA of PKI-infrastructuur voor verificatie van credentials.	Geaccepteerde trust anchors zijn nodig voor validatie van issuer DID en signing keys; kan PKIoverheid of GIS-VN CAs omvatten.
Delegatie / Delegation Credential	Bewijs dat een zorginstelling een dienstverlener bevoegd heeft.	Wordt opgenomen in Verifiable Credentials of Presentations; verifieerbaar door cryptografische binding.
PatientEnrollment	Inschrijving van een patiënt bij een zorginstelling.	Kan als VC of relatie-attribuut worden vastgelegd; gekoppeld aan patient DID.
VC-specifieke types	Credential types zoals `HealthcareProviderCredential`, ...	Elk type definieert veldnamen, cardinaliteit en validatieregels; gebruikt voor autorisatie en identiteitsverificatie.
Audience	Entiteit waarvoor een VP bedoeld is (aud claim).	Bindt een Verifiable Presentation aan een specifieke authorization server; voorkomt hergebruik bij andere servers.
JSON-LD context	Definitie van vocabulaire voor credentials.	Alle credentials maken gebruik van de gedeelde context; definieert namespaces (gis, schema, fhirnl), entity types, relatie- en attribuut-termen.
Endpoints publicatie	Mechanisme waarmee knooppunten endpoints van aangesloten zorginstellingen openbaar maken.	Nodig voor vindbaarheid via Query Directories; LSP registreert centraal, Nuts-knooppunten publiceren lokaal.
Token introspectie	Validatie van access tokens bij de AS conform RFC 7662.	RS kan aanvullende claims ophalen (URA, rolcode, bsn) afhankelijk van scope; DPoP binding check optioneel volgens Responding GtK.
Twiin deelnemer	Een Twiin deelnemer is een zorgorganisatie of dienstverlener die volgens de Twiin-afspraken gegevens uitwisselt met andere partijen in de zorg.	Binnen het Twiin-stelsel is een Twiin deelnemer een organisatie die formeel is aangesloten op het afsprakenstelsel en verantwoordelijk is voor het uitwisselen van zorggegevens volgens de Twiin-regels. De deelnemer kan de technische uitvoering van deze uitwisseling laten verzorgen door een GtK-beheerder, maar blijft verantwoordelijk voor de gegevensuitwisseling.
Care Service Directory (CSD)	Een adresseringsdirectory gebaseerd op het IHE mCSD-profiel waarin endpoints van zorgsystemen vindbaar zijn.	De CSD wordt gebruikt om systemen uit zowel het LSP- als het Nuts-netwerk te lokaliseren en adresseren. Wanneer een deelnemer een bericht wil sturen, kan het juiste endpoint van de zorginstelling of dienst automatisch worden opgezocht.
Holder (Verifiable Credential)	De partij die een credential bezit en kan presenteren aan een verifiërende partij.	In het stelsel kan de holder een zorginstelling, dienstverlener of individuele gebruiker zijn. De holder presenteert credentials of claims om zichzelf of een andere partij te

		authentiseren en te autoriseren binnen een transactie.
Issuer (VC /Claims)	De autoritatieve bron die een credential of claim uitgeeft over een subject.	De issuer kan bijvoorbeeld het CIBG (UZI/DEZI), het Handelsregister (KVK) of een organisatie zelf zijn. De issuer bevestigt de identiteit, kwalificaties of attributen van een subject, zodat deze verifieerbaar zijn door andere deelnemers in het stelsel.
Verifiërende partij/ Verifier	Een entiteit die claims of delegatiebewijzen controleert op geldigheid en authenticiteit, zonder op dat moment afhankelijk te zijn van de issuer.	De verifier kan een systeem van een dienstverlener of een zorginstelling zijn dat toegang wil verlenen tot gegevens of handelingen wil uitvoeren. Het controleert cryptografisch de geldigheid van gepresenteerde credentials of delegaties, waardoor realtime afhankelijkheid van de issuer wordt voorkomen en veilige gegevensuitwisseling mogelijk is.
Zorginstelling	Is een zorgaanbieder	Daar waar het begrip ‘zorginsteling’ wordt gehanteerd moet dit gelezen worden als ‘zorgaanbieder’, dus een organisatie met een URA.